ROMANIAN MILITARY THINKING

ROMANIAN MILITARY THINKING

INTERNATIONAL SCIENTIFIC CONFERENCE

PROCEEDINGS

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

NOVEMBER 2019
BUCHAREST

1ST EDITION

PUBLISHER
THE DEFENCE STAFF

CONFERENCE ORGANISING COMMITTEE

Chairperson:
Lieutenant General Daniel PETRESCU

Members:
Major General Vasile TOADER
Major General Teodor INCICAŞ
Major General Corneliu POSTU
Major General Dragoş-Dumitru IACOB

Secretariat:
Lieutenant Colonel Mircea BARAC
Lieutenant Colonel Adrian BOCHIŞ
Lieutenant Colonel Dan NISTOR
Warrant Officer Class 2 Katalin SĂVESCU
Iulia SINGER
Alina PAPOI
Diana Cristiana LUPU

DTP
Adelaida-Mihaela RADU

EDITORIAL OFFICE
Bucureşti, str. Izvor nr. 110, sector 5
Postal code: 050564
Tel.: +4021.410.40.40/1001731;1001732
Tel./fax: +4021.319.56.63
E-mail: gmr@mapn.ro
Web: gmr.mapn.ro

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

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

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

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

Printed
at Military Technical Publishing Centre
C ___/2019 B ____

ROMANIAN MILITARY THINKING

INTERNATIONAL SCIENTIFIC CONFERENCE PROCEEDINGS

SECURITY AND DEFENCE BETWEEN HISTORY, THEORY AND PUBLIC POLICIES

1ST EDITION

Print: ISSN 2668-7984, ISSN-I 2668-7984
Online:.....

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

NOVEMBER 2019

SCIENTIFIC INTERNATIONAL COMMITTEE

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

Larry WHITE, PhD, Senior Lecturer, University of Economics and Technology, Ankara, Turkey

Jaromir MARES, PhD, Professor, Brno, Czechia

Pavel OTRISAL, PhD, Professor, Brno, Czechia

Iulian CHIFU, PhD, Senior Lecturer, Multinational Operations Department, Strategic and Security Studies, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Ghiță BÂRSAN, PhD, BEng, Professor, Rector, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Gabriel RĂDUCANU, PhD, Senior Lecturer, Rector, *"Henri Coandă"* Air Force Academy, Brașov, Romania

Octavian TĂRĂBUȚĂ, PhD, BEng, Senior Lecturer, Rector, *"Mircea cel Bătrân"* Naval Academy, Constanța, Romania

Valentin DRAGOMIRESCU, PhD, Professor, Deputy Rector for Educational Activities, *"Carol I"* National Defence University, Bucharest, Romania

Ioana ENACHE, PhD, Professor, Dean, Command and Staff Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Laurențiu-Răducu POPESCU, PhD, BEng, Senior Lecturer, Air Force Department, Command and Staff Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Niculai-Tudorel LEHACI, PhD, Senior Lecturer, Deputy Dean for Research, Command and Staff Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Cristian-Octavian STANCIU, PhD, Professor, Director, Land Forces Department, *"Carol I"* National Defence University, Bucharest, Romania

Marius ȘERBESZKI, PhD, Senior Lecturer, Director, Air Force Department, *"Carol I"* National Defence University, Bucharest, Romania

Florin NISTOR, PhD, Professor, Director, Naval Forces Department, *"Carol I"* National Defence University, Bucharest, Romania

Marilena MOROȘAN, PhD, Professor, Director, Logistics, Finance and Accounting Department, *"Carol I"* National Defence University, Bucharest, Romania

Laurențiu GRIGORE, PhD, Professor, Director, Strategic Command Department, *"Carol I"* National Defence University, Bucharest, Romania

Daniel GHIBA, PhD, Professor, Deputy Dean for Research, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Dorel BUȘE, PhD, Professor, Multinational Operations Department, Strategic and Security Studies, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Cosmin OLARIU, PhD, Senior Lecturer, Multinational Operations Department, Strategic and Security Studies, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Cristian ICHIMESCU, PhD, Lecturer, Director, Defence Intelligence Department, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Ciprian IGNAT, PhD, Senior Lecturer, Multinational Operations Department, Strategic and Security Studies, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

Florian BICHIR, PhD, Lecturer, Multinational Operations Department, Strategic and Security Studies, Security and Defence Faculty, *"Carol I"* National Defence University, Bucharest, Romania

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

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

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

Mihail E. IONESCU, PhD, Professor, Director, Institute for Political Studies of Defence and Military History, Bucharest, Romania

Petre OTU, PhD, Scientific Researcher I, Institute for Political Studies of Defence and Military History, Bucharest, Romania

Vasile CĂRUȚAȘU, PhD, Professor, Deputy Rector, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Daniel-Sorin CONSTANTIN, PhD, Senior Lecturer, Deputy Rector, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Ioan VIRCA, PhD, Professor, Deputy Rector, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Mihai NEAG, PhD, Professor, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Dănuț MOȘTEANU, PhD, Professor, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Sorin PÎNZARIU, PhD, Professor, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Toma PLEȘANU, PhD, Professor, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Dorel BADEA, PhD, Senior Lecturer, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Marius MILANDRU, PhD, Senior Lecturer, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Romana OANCEA, PhD, Senior Lecturer, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Stelian POPESCU, PhD, Senior Lecturer, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Ioan-Gabriel POPA, PhD, Senior Lecturer, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Ioan-Dan POPA, PhD, Senior Lecturer, *"Nicolae Bălcescu"* Land Forces Academy, Sibiu, Romania

Adrian LESENCIUC, PhD, Professor, Deputy Rector for Scientific Research, *"Henri Coandă"* Air Force Academy, Brașov, Romania

Gheorghe SAMOILESCU, PhD, BEng, Professor, *"Mircea cel Bătrân"* Naval Academy, Constanța, Romania

Romeo BOȘNEAGU, PhD, Senior Lecturer, *"Mircea cel Bătrân"* Naval Academy, Constanța, Romania

Ioan BONDREA, PhD, Professor, Rector, *"Lucian Blaga"* University, Sibiu, Romania

Claudiu-Vasile KIFOR, PhD, Professor, Deputy Rector, *"Lucian Blaga"* University, Sibiu, Romania

Lucian-Ionel CIOCA, PhD, Professor, *"Lucian Blaga"* University, Sibiu, Romania

Adrian CURAJ, PhD, Professor, Director, Executive Unit for Financing Higher Education, Research, Development and Innovation, Bucharest, Romania

Ion POPA, PhD, Professor, University of Economic Studies, Bucharest, Romania

Cosmin DOBRIN, PhD, Professor, University of Economic Studies, Bucharest, Romania

Cezar VASILESCU, PhD, Professor, Regional Department of Defence Resources Management, Brașov, Romania

CONTENTS

DEFENCE RESOURCES MANAGEMENT

MILITARY HISTORY

SECURITY AND DEFENCE BETWEEN HISTORY, THEORY AND PUBLIC POLICIES

Lieutenant General Daniel PETRESCU
Chief of the Defence Staff

The *Romanian Military Thinking* international scientific conference took place in the context of two relevant anniversaries: 160 years of existence and evolution for the most important command structure of the Romanian Armed Forces – the Defence Staff, and 155 years since the first edition of the Romanian Military Journal, currently published by the Defence Staff under the name the Romanian Military Thinking.

The scientific endeavour organised by the Defence Staff, through the agency of the Romanian Military Thinking Journal, has proved to be valuable and useful. Valuable in terms of the quality of the scientific act promoted within such an institutional framework, and also the quality of the participants, but especially useful, due to its obvious contribution to the creation and development of a security culture, so much desired today by the whole of the Romanian society.

And if by security culture we understand raising awareness of the security challenges of a state, actively involving in solving them and supporting the actions carried out by state institutions in order to prevent and counter the threats to national security, a scientific conference is a good starting point in this respect.

The debates around the new regional or global security challenges will enable us to better understand the emerging risks and challenges that nations or the region as a whole is currently facing: terrorist threats, cyber vulnerabilities, various kinds of hybrid threats, which combine conventional and unconventional warfare methods, as well as all actions aiming at information manipulation.

We currently live in a hybrid combination paradigm, in which the classical military force intertwines with emerging threats – the revival of the phenomenon of confrontation between the great powers, the emergence

of the structural challenges to the international order, with regional and sub-regional manifestations, and the ongoing globalisation tendencies.

A problem that has arisen and needs a discussed solution is the way in which the information society uses violence, given that the unprecedented evolution of the IT technology has paved the way for information warfare. In this respect, the recognition of cyberspace as a domain of operations by NATO, in 2016, was a direct consequence of the increasing impact of cyber attacks on society.

The cyberspace is relevant to military operations, from the perspective of both defensive and offensive activities. For military commanders, the complexity of the cyber domain, overlapping with an already complicated, congested and contested land, air and sea operational environments, adds new challenges. However, a properly calibrated cyber resilience culture, one that is mission-oriented, and combined with *"classic"* resilience in a smart way, will help us plan operations based on consistent data in order to reduce operational risk.

Military strategy, as well as business strategy (and by this I mean technological revolution), must evolve in response to the constantly changing operational environment. The knowledge, understanding and, above all, the ability to react to all these challenges are prerequisites for preparing ourselves to face the demands of the future.

To sum up, the development of the security culture requires an inter-institutional approach. It is necessary for us to explain the new types of threats, risks and vulnerabilities that may have an impact at the individual, group, societal, national, regional or global levels. The civil society must be aware of these threats in order to be able to get involved, together with the authorised institutions, in identifying, preventing and controlling them. The construction of a modern society is based on individual and collective security. This must be the convergence point for national and international institutions, professional associations and non-governmental organisations.

The Romanian Military Thinking Conference is a very much welcome step on the path to meeting a real social need: strengthening our own security culture, fostering critical thinking and, last but not least, promoting this type of culture!

Therefore, I wish to take this opportunity to thank all those who have contributed in the smooth running and development of the conference, either through the organisational effort or through the direct contribution as a moderator, panellist or author!

ROMANIAN MILITARY THINKING CONFERENCE PROCEEDINGS

SECURITY AND DEFENCE BETWEEN HISTORY, THEORY AND PUBLIC POLICIES

PLENARY SESSIONS SYNTHESIS

The Defence Staff organised, between 06 and 07 November the current year, at the Palace of the Military Circle, the ***Romanian Military Thinking International Scientific Conference***, having as theme ***Security and Defence between History, Theory and Public Policies***.

The activity was scheduled in the context of the celebration of 160 years since the establishment of the Defence Staff and 155 years since the first issue of the *Gândirea Militară Românească/Romanian Military Thinking* journal appeared, being aimed at debating the issues of national security and defence, in the context of the latest developments in the security environment at regional and global level.

The event was attended by military leaders from the Defence Staff, representatives of the armed forces services, military academies, collaborators of the *Romanian Military Thinking* journal, professors and students in master and doctoral programmes, researchers within the Romanian Armed Forces, specialists, experts, academic staff and researchers from civilian educational and research institutions in Romania, specialists within the *Defence and Security Monitor* project, specialists and experts from other institutions belonging to the National Defence, Public Order and National Security System.

Four sections organised on eight panels, over 50 topics presented in plenary or parallel sessions, about 80 scientific papers submitted for publication and a generous theme – ***Security and Defence between History, Theory and Public Policies*** are the basic landmarks of the first edition of the *Romanian Military Thinking International Scientific Conference.*

Among the guests that delivered speeches were: His Excellency Sorin DUCARU, Ambassador – Director of the EU Satellite Centre, His Excellency Cristian DIACONESCU, President of the Centre for Foreign Affairs, Iulian CHIFU, PhD – President of the Centre for Conflict Prevention and Early Warning, Harlan K. ULLMAN, Chairman of the Killowen Group and Senior Advisor to the Atlantic Council, Washington, Antonia COLIBĂŞANU, PhD – Senior Analyst at Geopolitical Futures, Iulian FOTA, PhD – Head of the National Intelligence College, Professor Niculae IANCU, President I2DS2 – Integrated Intelligence Defence and Security Solution. Moreover, speeches were also delivered by guests from NATO Defence School, Rome, NATO School Oberammergau, and Joint Air Power Competence Centre, Kalkar, Germany.

The Defence Staff was represented not only by Generals Teodor FRUNZETI (r.), Mihail ORZEAŢĂ (ret.), Ştefan DĂNILĂ (r.) and Major General (ret.) Florian RĂPAN, but also by military leaders in activity such as: Major General Vasile TOADER, Major General Teodor INCICAŞ, Brigadier General Dragoş-Dumitru IACOB, Brigadier General Gabriel-Nicuşor ANGHEL, Brigadier General Nicolae MARIA-ZAMFIRESCU and Rear Admiral (Lower Half) Mihai PANAIT.

The foreign guests made their presentations in two panels within plenary sessions, namely the *Technological Revolution and Its Implications on the Security Environment* and *Trends regarding the Evolution of the Security Environment at Regional and Global Level*. Within the first panel presentations were made by Andrea GILLI, PhD, NATO Defence College, and Lieutenant Colonel G. W. PRONK, NATO Joint Air Power Competence Centre. During the second panel, Lieutenant Colonel Eric PINCZON Du SEL, Course Director within NATO School Oberammergau, made his presentation.

The conference had four sections, each having a distinct theme, as follows: *Military Theory and Art, Intelligence and Security, Defence Resources Management* and *Military History*.

Within the *Intelligence and Security* section, the main highlighted topics were: *Technological Revolution and Its Implications for the Security Environment*, *Evolution of the Security Environment at Regional and Global Level* and *NATO's Future – Geopolitical Challenges and the Imperative for Change*.

The *Military Theory and Art* section had as theme the *Contemporary Military Phenomenon: Challenges and Tendencies*. The section was aimed at highlighting the complex interaction between theory and practice in the military field, by reference to the main concepts and technologies that have led to the evolution of the military strategy over time, the main topics discussed being: the *Evolution of the Security Environment under the Spectrum of Hybrid Confrontations* and the *Technological Revolution in the Military Field and Its Implications for the Military Strategy*.

NATO'S FUTURE: GEOPOLITICAL CHALLENGES AND THE IMPERATIVE FOR CHANGE

One of the keynote speakers within the *Intelligence and Security* section was Mr. Harlan K. ULLMAN, Chairman of the Killowen Group and Senior Advisor to the Atlantic Council, Washington. A former officer in the US Navy with rich experience in the Vietnam War, H. K. Ullman is the author of several books, the most recent one being *Anatomy of Failure: Why America Loses Every War It Starts (Annapolis: Naval*

Institute Press). From his point of view, Romania can play a very active role in NATO, and the Romanian Armed Forces should focus on three directions, namely:

- Strategic concept: a *"hedgehog"* defence is needed in NATO and in Europe. Even if it has no intention to attack the West, what Russia is doing is to take intimidation and threatening actions. Therefore, it is necessary to draw up a new strategic concept that takes into account active measures, something that neither NATO nor the USA does. Romania can contribute to it, considering the prestige and influence it has gained due to the support provided in Iraq and Afghanistan;
- Reform: One of the reasons why NATO, in general, and the member states, in particular, are in difficulty is that bureaucracies are inefficient. For example, the US Armed Forces are going to pay half a billion dollars, a very high price, for a new pistol, and this is the result of bureaucracy. It is inefficient; thus, a serious reform is required at the Pentagon level, which has already been attempted several times. In Romania, however, there is now an opportunity for the reform to be much more efficient, compared to the money spent in this regard, which can be an example for the other states;
- The Romanian Armed Forces can play a decisive role in helping the Romanian society to make the transition from the industrial age of the 20th century to the information age of the 21st century. And it can be solved by developing a topical strategic concept. In Romania people are extremely intelligent and very well educated, trained in the information field, in computers, in software, crucial for the 21st century. The war is won with the brain, not with the bullet. The most important weapon available to a military man is his intellect. In this regard, Romania may be at the forefront of those who supply such a weapon. It is important to put into practice the power of these brains.

In His Excellency's intervention, Ambassador Sorin DUCARU emphasised that *"we live in a world where we are faced with a combination of emerging challenges and we must pay attention to the hard power-related aspects as well as to the traditional domains of military confrontation – air, land, sea, which are very important"*. However, there are at least two other areas having important roles of facilitators – cyber space and cosmic space. And in both of these areas we are dealing with what can be called the technological revolution and the effort to have available as much technology as possible, an aspect that influences the way we think, plan and act. These areas contain elements that blur a number of important

differences to which we were accustomed, for example, the difference between the concept of peace and that of war.

The entire international system, the international law after the Second World War, the balance of power and the strategic stability were based on avoiding war, avoiding the devastating confrontations that humanity witnessed in the 20th century. The UN Charter mentions peace promotion, with focus on self-defence, individual or collective, in the event of an armed attack. The difference between peace and war is made by the armed attack. The blurring boundaries are much more evident nowadays, especially since we are witnessing countless actions taking place under the armed attack threshold, as established in Article 10 of the UN Charter and Article 5 of the NATO Treaty. The fact that there are certain strategies, operations and techniques that are called hybrid, operating under this threshold, forces the limits of military planning, deception, and military response to this grey area.

In other words, at present, within the EU, there is an increasing concern for defence investments as well as for the development of real European military capabilities and for strategic autonomy. These developments need to be understood correctly and should not be seen as an EU action against NATO.

In the opinion of Ambassador Ducaru, the development of European capabilities, including those with a clear value of strategic autonomy, is relevant to the Alliance and does not represent something that NATO could or should replace.

An interesting topic related to the fundamental values of NATO was addressed by General (r.) Teodor FRUNZETI: *"The North Atlantic Alliance was and still is a reactive organisation, not a proactive one. What constituted the strength of the Alliance over time were some basic values such as the coherence, cohesion and solidarity manifested by its members throughout time.*

Lately, the Alliance has enlarged, and the interests of the component states are much diversified at present. Eastern European states perceive security threats differently than Western European states. This is one of the reasons why the B9 format was set up, made up of Eastern European states.

The current strategic concept dates from 2010, a different moment than the present one, previous to the annexation of Crimea and the intervention in Syria. Thus, there is another security paradigm, and NATO's strategic concept needs to be revised in the near future.

Regarding NATO's forward presence in the eastern flank, it should be achieved in a balanced way between north and south, as there are no major differences between the threats in the Baltic Sea area and the Black Sea area. Therefore, higher coherence, cohesion and solidarity are needed at the Alliance level".

The Director of the Centre for Global Studies within the *Lucian Blaga* University in Sibiu, Silviu NATE, PhD addressed a topical theme regarding the dilemma generated by the European Strategic Autonomy – ESA and the establishment of a European Army.

In his presentation, Mr Nate emphasised the fact that there is confusion within and outside the European Union regarding the concept of ESA. It entails, in principle, freedom of action and decision at EU level, together with the development of basic capabilities and the mobilisation of Allies and partners. The European Strategic Autonomy is justified by several aspects, such as increasing competition at geopolitical level, the effects of Brexit, divergences on EU foreign policy, hybrid threats, different perception of threats, increasing populism and nationalism etc.

Although ESA may be erroneously misinterpreted as the cause of a potential decline in the role played by NATO, in fact, the EU defence effort is meant to strengthen the North Atlantic Alliance and to encourage member states to cooperate in this area. *"In order to fully capitalise on the actually available potential, the EU should renounce its strategic ambiguity and focus on developing defence capabilities through the European Defence Fund and PESCO"*, Mr Nate considered.

General (r.) Ştefan DĂNILĂ, a former Chief of the Defence Staff, revealed that at the Chicago NATO Summit in 2012 NATO's utility was addressed. It was the period when the Russian-American relations were reset, under the circumstances in which President Vladimir Putin seemed to take a step back into the second echelon. On the other hand, 2009 should be considered as the year that represented the beginning of the reform of the Russian Armed Forces. It was not just about the intervention in Georgia, but something more. It was visible, first of all, in the morale of the Russian military, who were no longer having problems with the payment of salaries. Moreover, the replacement of the outfit was another message of force transmitted from the Kremlin.

After the 2013 ZAPAD exercise, it became clear that Russia was a danger, but, unfortunately, the threat posed by Russia was seen differently from London, Berlin or Paris. General Philip Breedlove, the Supreme Allied Commander Europe, expressed his concern at that time regarding Ukraine, given that it was a divided state in terms of religion, culture and education.

Following the unclaimed military actions that preceded the annexation of Crimea by Russia, the idea of hybrid warfare was included in the US defence strategy, in 2015, General Dănilă pointed out.

The need for the North Atlantic Alliance to adapt to a rapidly changing security environment was the topic addressed by Major General Vasile TOADER, who reminded the audience that a simple scan of the current security environment detects a certain increase in its complexity, instability and uncertainty, and there is no reason for us to believe that there is a tendency to relax in the near future. Conventional, hybrid and asymmetrical threats are interconnected in different ways and patterns, from the Baltic Sea through the Black Sea, the Mediterranean Sea to the North Atlantic Ocean, being generated by state and non-state actors, or by failed states belonging to the area of instability surrounding Europe having ramifications in the Middle East and North Africa. With the illegal annexation of Crimea in 2014, the recrudescence of the Russian Federation foreign policy, a force policy, has been a fact that no longer needs to be demonstrated, and the projection of instability at all levels has become the instrument preferred by the Kremlin in the intention to change the global status quo in its favour.

The measures to counter these de facto states of affairs have already been initiated, both at the Alliance and the member states level, and they are generally focused on intensifying deterrence and strengthening NATO's posture, by ensuring a forward presence in the eastern flank. Beyond any concrete measures, the power of the Alliance lies in the unity, solidarity and cohesion of its members, and these are the values that must be protected at any cost. Romania has understood that defence begins at home, and in this respect, it has allocated a budget that would ensure predictability in terms of the military body modernisation, while meeting all the operational commitments assumed as an Alliance member state and as a stability pillar in this part of Europe.

TECHNOLOGICAL REVOLUTION AND ITS EFFECTS ON THE SECURITY ENVIRONMENT

The first speaker within the panel was Iulian CHIFU, PhD, who emphasised the link between unconventional threats and the new types of conflicts having a hybrid nature in the 21st century:

"The evolution of international relations, the turbulence and acceleration of both integration and fragmentation in the International World Order lead to unexpected and unconventional forms and types of threats to national and international security. Some come from the technological development, some from the impact of those technologies on our societies, some others from the rise of populism and identity relevance, and last but not least, from our own minds

and perceptions that are influenced dramatically by our preconceptions and easiness of the rational thinking. All these have a huge impact on the new threat assessment, on the security and defence of a nation. That is why those facts need to be explored, known and approached in a scientific and comprehensive manner in order to prevent strategic surprise in such areas and the emergence of new types of conflicts.

In the case of social media, the impact of propaganda, disinformation and information warfare is very well known. Less known and studied are the indirect threats to security, namely the impact of the social media on political security and societal security. The means of social media influence on society are several, and the negative side effects should not prevent the huge positive effects of this tremendous technical achievement.

Therefore, societal security and political security have a direct impact on hard security, starting from recruitment, through education and training, to the moment future actions have to be planned, and scenarios have to be identified.

Funding security needs is also related to a clear perception of the evolution of security threats and concerns as well as to the general understanding of the mistakes we, the today people, all make, and of the fact that we are all the subjects of these collective mistakes and disinformation".

Andrea GILLI, PhD delivered a presentation on the topic of *NATO Transformation in the Context of Artificial Intelligence Development*. In his presentation, Mr Gilli started from the question whether Artificial Intelligence strengthens or weakens NATO power, considering the fact that it contributes to strengthening not only the Alliance but also other state or non-state actors, which could lead to the emergence and escalation of many conflicts. According to Andrea Gilli, the technological revolution in military affairs is, in general, evolutionary. The more intense the technological change is, the more difficult the process of adaptation would be, resulting in slower change effects. Change requires countermeasures as well as tactical and operational adaptation. This process is based on information. However, can we trust the information we have? We need to ask ourselves who provides the information and why so that we can discern between data, intelligence and sabotage. Identifying, acknowledging, anticipating and addressing vulnerabilities require time and resources. The more responsibilities are entrusted to Artificial Intelligence, the more important the responsibilities of humans would be.

According to Mr Gilli, NATO should constantly experiment and exploit new technologies in order to strengthen its force structure. It should be done at a pace

that is not too slow, as it would mean lagging behind, and not too fast either, as it could lead to failure.

With regard to the technology that can influence or facilitate the geopolitical analysis, an interesting presentation was delivered by Antonia COLIBĂȘANU, PhD, senior analyst within Geopolitical Futures.

In her opinion, innovation is usually associated with technological progress. In terms of information analysis, progress stems from the challenges faced by analysts in determining the usefulness of information, considering the available data transformed into information. For the geopolitical analysis – employed in the strategic decision-making process, progress is determined by the acknowledgement of the details that influence the status quo at the national level and, in particular, those elements that may affect the state's security needs. Therefore, it is important to understand what constitutes *"change"* and what does not, in relation to information analysis – and how it can help (or limit) our ability to point out the importance of change, strategically.

We are currently dealing with what will be next in terms of innovation. When we talk about technology and what it brings about, we can see how the workforce has already changed in human capital, in human resource. Society consists of personal networks, communities of people, the community being at the root of the way society changes as well as the way society introduces innovation. That is why, at present, we have to deal with a different map, not a physical one, which explains the limitation of actions (for example, the role of mountains and seas in military actions). As society changes, the map changes too, based on networks. Such a map also shows the possible centres that could cause problems in the future world. Therefore, it is important to have a general conceptual framework for the way we interpret *technology as a factor that influences information collection and analysis processes* – and, thus, for the way these elements are linked and determine innovation in the decision-making process at strategic level.

The relationship between information and the concept of security (national and international) is aimed at explaining and promoting common defence policies, resulting from the decisions made not only at the NATO summits in the past decade but also at the European Union level. A new arms race, asymmetrical threats, cyber security or the impact of Artificial Intelligence on security are just a few of the issues that have led to the revision of the priorities in the field of security and defence of the actors on the international scene.

Lieutenant Colonel G.W. PRONK made a presentation on the topic of the *Challenges Posed by Hypersonic Operational Threats*. He began his presentation with a very interesting discussion regarding the way in which air defence systems were integrated within NATO during the Cold War, mentioning that during the last decade of the previous century it was a change in NATO strategic posture, generated by the reduction of ballistic threats. In the centre of current threats there are hypersonic capabilities, namely missile systems that can reach extremely high speeds so that this type of vectors can exceed the Earth curvature (e.g. Kinzhal system developed by the Russian Federation). There are several models to respond to such type of threats, all having three basic elements: sensor – interceptor – network technology. The perfect functioning of each element is essential: if the interceptor is misaligned or its agility decreases in time or the sensor is not in a correct position, the counter-attack may be compromised. However, the most difficult aspect is represented by the total coverage of the territory in terms of defending it against such threats, the necessary capabilities required for such an approach being extremely expensive.

The impact of disruptive technologies on the operational environment was a topic addressed by Brigadier General Dragoş IACOB. *"The OODA Cycle, Observe-Orient-Decide-Act, for which Colonel John Boyd became famous throughout the world, is the one that provides the OODA act in relation to the adversary's decision-making cycle. Due to this cycle, our decision-making process is getting shorter, so we can surprise our opponent and act while he is barely orienting. With the help of disruptive technologies, the cycle of action will become shorter and shorter.*

We can use this prototype war, despite the ethical and technological constraints, by combining, for example, the activity of satellites using ISR (Intelligence, Surveillance, Reconnaissance) technology with autonomous vehicles and command and control exercised from a remote location, according to an algorithm previously approved by human beings.

As for the challenges, we can say that we need to be aware of a number of possible developments. First of all, the change of the operational environment will probably cause us to look at this type of operations as belonging to the multi-domain type, acting not only in the land, maritime and air domains but also in the cosmic space and in the cyber space, taking place in an electromagnetic spectrum. It is thus necessary to figure out what to do to dominate in such an operation.

Moreover, interoperability is extremely important, even if we consider only one reason: which is the way we can act alongside an ally or a partner that is more technologically advanced. Because the common denominator is represented,

in this case, by the least technologically advanced partner. This aspect, in itself, is a challenge. Therefore, education and training are essential to understand and use/deal with such technologies. It is extremely necessary to focus on the way we approach innovation and to consider the requirements, in terms of knowledge acquisition, for the future military leader to be competent and to win tactical victories".

TRENDS IN THE EVOLUTION OF THE SECURITY ENVIRONMENT AT REGIONAL AND GLOBAL LEVEL

Diplomacy and International Relations in a Constantly Changing Security Environment was the topic addressed by His Excellency Cristian DIACONESCU, Ambassador. According to the former foreign minister of Romania, international relations are currently under pressure due to several factors, such as: immigration and integration pressures, climate change, resource depletion, challenges arising from cyber threats and crimes, growth, scale and impact of terrorism and organised crime.

From a political point of view, threats are perceived differently by citizens, depending on the region in which they are. Thus, if for the citizens in the Wider Black Sea Region, the main danger seems to come from Russia, for the citizens in Central and Western Europe, the main dangers are represented by illegal migration, terrorism, cyber-attacks etc. Such threats have become transnational and globalised in their nature. In order to combat them, coherent national and regional policies are necessary as well as effective cooperation between the states that are part of a certain economic or military bloc.

Iulian FOTA, PhD emphasised the fact that, currently, there is a state of degradation in the international security environment, under the circumstances in which the trend is for the great powers to dominate certain areas of interest. Most likely, in the near future, we will witness the renegotiation of the power poles and the transition from a unipolar to a multipolar international system. The most relevant example in this respect is China, which has lately become the greatest economic power and seeks to achieve supremacy in all the fields, the military one included. In the Middle East, there is no sign for the stabilisation of the security situation in the next 10-15 years, and Russia has played an important role in this area. Moreover, Russia, through its actions, practices a policy of intimidation in the Wider Black Sea Region. During 2019 Russia practically *"confiscated"* a quarter of the Black Sea through the military exercises it conducted in this area.

Moreover, the great powers invest in technology, in information and mass manipulation. Against the mentioned background, we will witness unforeseen and unpredictable decisions, made without consultations with partners. An example in this regard is the US withdrawal from Syria. The US partners learned about it from Twitter, which put them in a delicate situation.

Stopping the EU enlargement is another sign that future scenarios are difficult to anticipate. The problem is that we are reluctant to acknowledge that we are facing a security deficit, and this is the result of a lack of security culture at the level of both political leadership and society.

The presentation made by Lieutenant Colonel Eric PINCZON du SEL focused on the topics of STRATCOM and INFOOPS in NATO acceptance. The information environment is a virtual battlefield for STRATCOM and it is constituted not only by the information mix but also by the actors participating in it – individuals, organisations, networks, as well as by the cognitive, virtual or physical spaces in which the exchange of information takes place. The ultimate goal of NATO STRATCOM is to achieve the final goals of NATO policies, and in line with this idea a first-rate objective is to protect and promote the key messages of the Alliance. STRATCOM is seen, at the Alliance level, as a continuous process rather than a capability. This process must promote a better understanding of the communication function, beyond the traditional media approaches. INFOOPS, on the other hand, is not a communication capability, such as public relations or PSYOPS. They rather represent a functional integrator, which is aimed at creating effects in the information environment and, ultimately, at supporting the decision-makers in meeting the proposed objectives. A list of the capabilities, tools, and techniques used to achieve the desired effect in the information environment would include PSYOPS, electronic warfare, CIMIC, public relations, social media, KLE – Key Leaders Engagement, cyber-attacks, physical damage etc.

DEFENCE RESOURCES MANAGEMENT IN ALLIED CONTEXT

The pace of changes and transformations entailed by the new revolution in military affairs has accelerated in the past few years, especially after the terrorist attacks on 11 September 2001. Although the essence of war has not changed, the forms and processes of military action, including those of armed war, have evolved, in dependence on the characteristics of the strategic security environment, forces, means, weapon systems, policies and strategies. Under such circumstances, the *Defence Resources Management in Allied Context* section equally covered

the human, material, information and financial resources management, the main ideas emerging from the debates being as follows:

- human resource is the most important asset because it enhances the entire armed forces activity. This resource should be thoroughly planned as its impact on any activity is decisive;
- with regard to the information resources, in addition to the strategic utility of this type of resource, the activities of ensuring access to them as well as the related counterinformation assurance should be taken into account, as they require considerable financial resources;
- financial resources are very important and they should be ensured for the employed personnel as well as for the procurement of the equipment and logistics necessary for the activity of the Ministry of Defence.
- defence capabilities depend on the quality of the weapon systems that contain, in an integrated manner, products, subassemblies, hardware, software, facilities, people and basic processes, quality that is best achieved through an integrated systemic approach throughout the whole life cycle of the weapon product/system.

In the presentation made by Professor Niculae IANCU, *Development Perspectives on European Military Capabilities*, it was argued that EU initiatives were launched not only to stimulate defence cooperation but also to demonstrate, in a crisis period of time, that the Union can make progress (despite the Brexit referendum, the foreign policy of the US President, the maximum migration rate and the rise of Euroscepticism/populism). Considering the current state of affairs, the prospects for European defence capabilities remaining poor, the question arises as to whether it is possible to have a politically integrated Union without having a credible defence policy to defend it. Under the strategic autonomy motive, the EU started, with its global strategy in 2016, a new attempt to define its global role. As a result, the European Commission new approach is aimed at: (1) technological autonomy through ***massive investments in defence research*** (at EU level); (2) integrated architecture for the ***development of defence capabilities*** (led by Brussels); (3) the EU should become a global actor that competes even with the USA.

The discussions on the European Defence Fund revealed the development trends for future European defence capabilities. A stronger European defence requires for the member states to purchase, develop and jointly maintain the full spectrum of land, air, space and maritime defence systems. As the European defence market suffers from fragmentation and insufficient industrial cooperation, more efficient use of public money is required, and a stronger industrial base could

be achieved by strengthening the single defence market, reducing duplication and improving the EU defence industry competitiveness. The Commission provides a *European Defence Action Plan*, which focuses on capability needs and supports the European defence industry.

At the level of strategic thinking, ideas have evolved over time, in terms of both the phenomenon of revolution in military affairs and the geostrategic context of the moment. Romanian military leaders made important decisions at crucial times. The way in which the Romanian school of thought has evolved over time is a useful history lesson that deserves to be known by the present generation. Some of the questions were answered in the discussions within the *Military History* section. The main topics for debate were: *Romanian Military Thinking – from Theoretical Concepts to Operational Practice*, as well as *Main Decisions of Some Romanian Military Leaders*.

As a conclusion, it can be said that the debates during the conference highlighted the fact that the first part of the 21st century is under the sign of exploration. Following it, the military science will have to redefine the scope and manifestation of each of the three levels of military actions, the principles and norms that will govern the war, the campaign, the operation, the battles and the armed clashes, the forms, the methods and the procedures for their preparation and conduct. The knowledge, understanding and, above all, the ability to respond to all these challenges are necessary conditions for preparing to meet the future requirements.

A RETROSPECTIVE GLIMPSE ON THE CONFLICT IN UKRAINE

Alexandru HERCIU, PhD
Senior Lecturer, "Carol I" National Defense University, Bucharest

The Crimean crisis erupted after President Viktor Yanukovych's departure from power following the 2013-2014 anti-government protests. Its trigger was the time to repeal the law on the status of regional languages, by which several languages used in Ukraine were removed from official use. The involved actors were, on the one hand, the Russian-speaking groups that opposed the new political changes in Kyiv and wanted the annexation of Crimea by Russia and, on the other, the Ukrainian groups and the Crimean Tatars, who supported the Euromaidan movement.

The analysis, first of all, requires understanding the key concepts and threats other than the conventional ones that have arisen in Ukraine for the practical implementation of Russia's strategy and policy of protecting the divided Russian-speaking compatriots, restoring the Russian civilization and reconstructing the Russian world (Russkiy mir).

Considering the importance given by global, European and national security institutions to this geopolitical conflict with perverse geometry, we intend to present this study from the perspective of the following conceptual elements: the historical context; political and strategic assumptions; the physiognomy of the military actions carried out in a hybrid context; the analysis of the characteristics of the hybrid type conflict in the understanding of the Russian Federation.

Keywords: conflict in Ukraine, annexation of Crimea, hybrid conflict, national identity, Russian Federation.

THE HISTORICAL CONTEXT

In an attempt to understand Russia's foreign and national security policy, political-military analysts have made inroads into the country's history. It is appreciated that, after the fall of the Soviet Empire, Russia is looking for a new identity and a strategy to secure it. In the specialists' opinion, although today Russia can no longer have the same geographical scope, it retains its historical feature of the Empire – a multi-ethnic and multicultural state.

At the same time, also from a historical point of view, it can be stated that, in Russia, the cohabitation of the peoples is not the result of migration, but of the advance of the Russians on the territories of other peoples. Of these, in 1992, some emancipated themselves, while others retained their status as vassals of the new Russia. These answers also suggest a particular uncertainty of the Russians in their self-definition as citizens[1].

On the attempt to define a national identity and to reflect this effort in Russia's foreign policy, there are three approaches and currents of thought: 1. Pro-Western liberalism, 2. Realism (or the balance of the great powers) and 3. Nationalism (with its two branches: a. Neo-imperialism and b. Ethnic nationalism). After 1992, the succession and the reflection of the influence of these currents of thought in the foreign policy of Russia are presented as follows[2]:

- 1992: liberalism;
- 1993-2000: realism;
- 2001-2002: realism with some influences of liberalism;
- 2003-2008: realism;
- 2009-2011: realism and liberalism;
- 2012-2013: realism;
- 2014: realism and nationalism.

In order to exacerbate and gain the needed support to embrace nationalism by the people on the borders of the Russian Federation but also from the former Soviet states, Putin resorted to four key concepts: 1-Compatriots, 2-*Russkiy mir* (Russian world), 3-Russian civilization, and 4-The Russian people divided. These key

[1] Mihaiu Mărgărit, *Ucraina şi războiul hibrid, în tentativele Rusiei expansioniste ale Moscovei de revenire a ei la masa marilor decizii ce privesc geopolitica mondială*, Pulsul Geostrategic, No.175, Saturday, 20 September 2014, see www.ingepo.ro, retrieved on 20 August 2019.

[2] Igor Zevelev, *Russian National Security and Foreign Policy*, lecture delivered on 23 October 2014, *"George C. Marshall"* Centre for Security Studies, Garmisch-Partenkirchen, Germany.

concepts, as well as the threats other than the conventional ones manifested in Ukraine, have contributed to the implementation of Russia's strategy and policy of protecting the divided Russian-speaking compatriots, restoring the Russian civilization and reconstructing the Russian world *(Russki mir)*.

In the case of Ukraine, these threats evolved in support of the hostile political movements against the pro-Western regime and the EU, the penetration of strategic industries, the influence of Russian energy suppliers in the governments of some states, the radicalization of the pro-Russian ethnic movements and the creation of enclaves, and cyber-attacks. All this happened under the pressure of a conventional military force deployed on the border, meant to discourage and prepare to intervene militarily.

Regarding the security of national identity, Russia's strategy is clearly explained by Ilya Prizel, in *National Identity and Foreign Policy (1998)*: *"While the redefinition of national identities is, in general, a gradual process, in situations of persistent crisis, even identities well established ones can change at a remarkable rate, and the collective memory of citizens can be ‹‹rearranged›› quite quickly"*[3].

Therefore, post-Soviet Russia is trying to find a balance between its multinational state, the fervent nationalism of its subjects and a more recent constraint: Russian nationalism. The Russian nationalism is stimulated from the Kremlin, both inside and outside the current geographical area of the state[4].

Russia's game and foreign policy are aimed at maintaining the non-involvement of states within its sphere of influence in military alliances such as NATO or EU integration, which President Vladimir Putin considers to be threats to Russia.

In this direction, President Putin stated on 18 March 2014: *"With Ukraine, our Western partners have crossed the line... After all, they were fully aware that there are millions of Russians living in Ukraine and Crimea... Russia itself was in a position it could not renounce. If you compress the arc to its limits, it will stretch firmly"*[5].

The Western response was to support Ukraine, sanctions against Russia and increase NATO's collective defence capabilities. NATO and the EU have responded to the security environment challenges generated by the hybrid war that Russia has unleashed in Crimea: offensive information operations, cyberwar, undermining of local administration, media control, infiltration of special operations forces, deployment of conventional forces in the vicinity of the border. Under these conditions, the *Readiness Action Plan* and the creation of the *Rapid Reaction Force* are two reference elements in the equation of NATO's fundamental mission.

[3] *Ibidem.*

[4] Mihaiu Mărgărit, *loc. cit.*

[5] Igor Zevelev, *The Russian World in Moscow's Strategy*, Center for Strategic & International Studies, see www.csis.org/analysis/russian-world-moscows-strategy, retrieved on 4 August 2019.

These measures are intended to ensure that NATO has the right forces and the right equipment, at the right place, at the right time. Besides, conducting more than forty military exercises only in Eastern Europe in 2014 shows that the Member States are sending a clear signal not only to the Alliance and partners in the region but also to Russia.

The Alliance must be prepared for such an undeclared type of war in Europe, clarifying in what situations it can invoke Article 5 of the Washington Treaty: economic, ecological, psychological, or cyber aggression. The introduction under the Article 5 of the fifth dimension of the battlespace, the cyber dimension (next to the terrestrial, naval, aerial and cosmic dimension) will allow a collective response if the virtual space is attacked in the future by the Alliance hostile forces.

However, the Alliance cannot fight alone in a hybrid war but needs the participation of other international bodies such as the EU and the OSCE that are also targeted by hybrid threats. The model of the war launched by Russia comprises components of a different nature than the military one, which also calls for economic, diplomatic, political or information *"campaigns"*. In this context, the states in the area of influence of Russia have the responsibility of preventing and preparing the campaigns of response to its hybrid methods, through good governance and – critical – by adequate management of the rights of minorities[6].

The political-military analyst Mihaiu Mărgărit identifies, beyond these historical considerations, other elements that justify the hybrid war unleashed on Ukraine. Russia's strong arguments in its foreign policy are Russia's position as a permanent member of the UN Security Council; the wealth of its mineral resources; the power of the armed forces, especially its nuclear arsenal. All these are *"support pillars"* on which Russia has built its diplomatic instruments. Then, the most important vectors of foreign policies of the great powers were and are tightly anchored in a very complex international geopolitical context. It is marked by the escalation of terrorist threats, as well as by the global financial crisis and the severe and long-term economic recessions, especially in the European space. They were associated with a significant set of specific challenges, risks, and threats that reinvigorated some frozen conflicts.

POLITICAL AND STRATEGIC PREMISES

Russia has therefore launched a set of asymmetrical threats against this country in an unconventional, hybrid war. According to the same author, the strategic war plan was implemented in two phases: one subtle, one of wear and collapse inside

[6] Heidi Reisinger, Aleksandr Golts, *Russia's Hybrid Warfare – Waging War below the Radar of Traditional Collective Defence*, Research Paper No. 105, November 2014, p.11.

Ukraine, and one of strength and visibility. The latter one targeted actions, gradually, and, paradoxically, without clues and warnings to alert of changing the situation and existence of a strategic hybrid war plan, developed and triggered in its sensitive parts, long before:

- Undermining the activity of the Ukrainian government, which according to the author represents a real threat to an open international system, based on the respect of the sovereignty and territorial integrity of the states; it is an interstate conflict and not an internal conflict in Ukraine, as it tries to prove Russian propaganda. It is appreciated that one of the most effective means of exerting pressure on the Ukrainian government since 2008 has been the dependency on Russia's energy resources;
- Speculation of the attitude of the population and the demographic, ethnic, and religious structure of Ukraine as well as the perceptions of the public opinion regarding the process of EU integration;
- Use in its favour of corruption in the national security system of Ukraine;
- Crumbling and annexing Crimea without shooting any firearms, the population assisting harmlessly in the troop of *"green men"* with missions to destabilize public life and state structures, masked military, informally *"stateless"* – a new invention of hybrid warfare. They joined the local militias, replacing the deployment of traditional invasion forces, consisting of aviation, armoured vehicles, or tanks. Later, they became *"deterrents"*, infiltrating the eastern part of Ukraine, bled by pro-Russian separatist insurgents, acting with them and others *"sent for humanitarian purposes"*;
- Organizing, equipping with armament and military infantry equipment, even with sophisticated military system and training the formations of these insurgents, who have ruled for secession – Russia is known to have provided sophisticated armament, armour, artillery, and BUK-type anti-aircraft defence systems to separatists (which shot down Malaysia Airlines Flight MH17);
- The implementation of the other force components of this strategic war plan determined and favoured by the moment chosen by the pro-European supporters to trigger the Euromaidan movement. Moreover, regarding the moment of the outbreak of hybrid warfare, in his February 2014 article, Gerasimov quotes Russian military theorist Georgii Isserson who stated that mobilization does not take place after a war has been declared, but *"begins unobserved long before that"*[7]. In the case of Ukraine, the plan implementation took place in a situation of economic weakness of the EU,

[7] Ana Stan, *Rusia a ridicat războiul la rang de artă* (article), 02.09.2014, see adev.ro/nb9y9f, retrieved on 30.03.2019.

controversies regarding its existence and a considerable increase in the number of Eurosceptics. This context gradually generated an unexpected and confusing, complicated situation. Thus, the main objectives were dissipated in a variety of violent confrontations between people and categories of the population having different political, social, professional, criminal, ethnic, religious backgrounds. After a period of physical and moral wear and tear, the movement appeared to have escaped the control of the initially proposed purpose, gaining the configuration of confrontations of maximum violence, bloody, dominated by manipulation, propaganda and multiple other components of psychological operations with unknown authors;

- Conducting intensive psychological operations. (It is surprising how fast and well the referendum was organized in Crimea, as well as the speed with which the local government structures passed into the legislative and administrative subordination of Russia. Similarly, two days after the Crimean referendum, after the legal formalities had been completed, the new local authorities already installed and delivered the first 80,000 Russian passports);
- Launching offensive cyber-attacks on official diplomatic and government information systems. It is alleged that since 2010 Russia has been spying on Ukraine by contaminating with the help of an extremely aggressive computer virus *"Snake"* official targets for access to Ukrainian state secrets[8];
- Motivations related to belonging to the Orthodox community were appealed, forcing the creation of a *"fallacy of a religious nature"*. This quarrel led to speculation, but also street protests, even with the unorganized participation of the Orthodox church's servants of all three branches existing on the territory of the country – the Ukrainian Orthodox Church, under the administration of the Moscow Patriarchate, the Ukrainian Orthodox Church with the Kyiv Patriarchate, the Autocephalous Ukrainian Orthodox Church;
- Carrying out *"actions to incite violence"*, aimed at both the pro-European supporters, creating *"confusions"* between options, as well as at the law enforcement, firing at maximum the general atmosphere of the Maidan.

Thus, we find that such types of operations are used to induce confusion or to consolidate favourable attitudes and behaviours for the initiator's goals. These are sometimes combined with clandestine actions or tactics under the false flag. Also, note that the target audience can be, as we have pointed out, groups and individuals, organizations and, in the case of Ukraine, especially the government.

[8] *Ibidem.*

THE PHYSIOGNOMY OF THE MILITARY ACTIONS CARRIED OUT IN A HYBRID CONTEXT

The conflict in Ukraine is an effective and surprising combination of military and non-military, conventional, unconventional, and irregular components as well as other types of tools such as cyber and information operations. Analysed individually, none of these components is new, but the combination and orchestration of the various actions that achieve surprise and create ambiguity make it extremely difficult to find the right solution, especially for multinational organizations operating on the principle of consensus[9]. The plan that Moscow implemented in south-eastern Ukraine was as follows: it concentrated its conventional and unconventional armed forces on the border to demonstrate its strength. Then it started supporting separatists by sending armaments and trainers to the conflict area. In the end, it invaded Ukraine directly but undercover.

In the first part of the operations in the Donetsk and Luhansk regions, the Russian special forces acted as instructors and experts in the use of sophisticated military systems. When the Ukrainian army began to push back the separatist forces, threatening to close the border with Russia, Russia sent undercover forces across the border to support the separatists. It is estimated that between 3,000 and 4,000 Russian soldiers fought in Ukraine, forming part of battalion units, deployed from four airborne divisions, together with the 18th Brigade[10].

Russia started, in 2013, to create a well-equipped, well-trained and modern structure capable of being deployed in the region, organized in:

- Airborne forces – about 20 battalions (four divisions, five brigades);
- Marine infantry (four brigades, eight independent regiments);
- Special forces brigades (GRU Spetsnaz);
- 3-4 units of elite land forces;
- Air and naval support.

Ukraine had 41,000 servicemen in the ground forces, of which 20,000 were in combat-ready units (on paper, but, in reality, around 6,000). The situation in which the Ukrainian army was found was a tough one because its units were framed by conscripts during the last months of military training, before moving to a professional army based on volunteering, the authorities delaying their demobilization. The morale of the military was low, many of them trying to escape military service or surrender, except for the battalions of volunteers subordinated to the Ministry of Internal Affairs that had good morale but a shallow level of training.

[9] Heidi Reisinger, Aleksandr Golts, *op. cit.*, p. 3.
[10] *Ibidem* p. 5.

However, in order to avoid the loss of other territories besides Crimea, Ukraine had to act. Thus, in April 2014, it launched the *"anti-terrorist"* operation, using conventional regular forces against unconventional and paramilitary forces, which make the use of armoured, artillery and air-defence useless. This mode of action was considered a great military and political error, because the conventional forces are not prepared to fight paramilitary forces, in an urban war, among the civilians used as human shields. This type of conflict requires the intervention of forces specially prepared for fighting in urban areas.

Given that the Ukrainian troops involved in the war amounted to about 50,000 people (comprising all units and military formations of reservists, volunteers, special forces, the Ministry of Internal Affairs) it proved extremely difficult if not impossible to achieve an efficient command and control system, a fact confirmed by the divergences and contradictory opinions of the commanders of the forces involved in the operation[11].

In the paper *Russia's Hybrid Warfare – Waging War below the Radar of Traditional Collective Defence*, the analysts of the research division of the NATO Defence College in Rome identified five key aspects of Russia's approach that are interconnected and overlapping[12]:

- *Conducting actions in an apparent legality*: (war was not declared, Russia was not officially a party to the conflict, the invasion of eastern Ukraine by thousands of combat-equipped military took place while they were officially on leave; annexation of Crimea came after a referendum that did not meet international standards and the distribution of Russian passports in eastern Ukraine was encouraged by the distribution of food packages, to increase the number of Russian citizens who had to be protected);
- Conventional military component: as of February 2014, Russia began to deploy conventional forces comprising between 30,000 and 40,000 soldiers on the border with Ukraine for the so-called unannounced inspections (so prevalent during the Soviet period and reintroduced in 2013) and the conduct of some extensive military exercises. A few weeks later, another such inspection was conducted in the Central Military District, involving more than 65,000 servicemen, 177 aircraft, 56 helicopters, and 5500 vehicles and armoured vehicles, with military units being able to be deployed in less than 72 hours. In order to avoid the involvement of international observers, Russian officials argued that units execute combat instruction in unknown areas by performing deployments over distances of more than 500 km,

[11] *Ibidem*, p.10.
[12] *Ibidem*, pp. 3-8.

per units, and that they do not perform joint manoeuvres that contravene the provisions of the Vienna Document[13];

- *Putin's masked ("little green men")*: little green men (or *"polite people"* as Putin likes to call them) are Russian special forces who act as *"local security forces"*, without wearing badges. In Crimea, the presence of these unidentified special forces was a means of psychological warfare and a useful tool for voting the independence referendum;
- *Obtaining the support of the civilian population*: the technique used consisted of the support of the local Russian minority, speculating dissatisfaction with the local political leaders. The action was labelled as one of *"protection of Russian compatriots outside the border"*, later transformed into a militarized separatist movement. For the Ukrainians, the war in the east has raised many problems, because it is a combination of actions carried out by paramilitary groups and conventional military forces. It is appreciated that the transition from guerrilla warfare to classical military operations is a rare phenomenon because both sides of the conflict avoid direct military confrontation;
- *Propaganda*: In May 2014, President Putin rewarded with medals about three hundred journalists, camera operators, and technicians who were involved in reporting events in Crimea, all working at state-owned media companies. Independent television channels have been marginalized, with the possibility of accessing them only on the Internet. Unlike the war in Georgia, Moscow has been able to effectively use the television channel *"Russia Today" (RT)*, a fast-rising station nicknamed by the German magazine *Der Spiegel* the *"*[Russian] *Ministry of Media Defence"*. The role that this television station played in the conflict in Ukraine was not only one of presenting the position of Russia, but also one almost declared of misinformation, according to the statements of the chief editor Margarita Simonyan: *"objectivity has never been my goal"*. Information and media are also considered weapons: *"... in time of peace an international channel is not absolutely necessary. However, in wartime, it can be crucial"*[14].

[13] *The Vienna Document (VD)* refers to measures to increase confidence and security (CSBM) in the OSCE area. The negotiations on the CSBM measures were held in Vienna in 1990, resulting in the *1990 Vienna Document*, which was subsequently revised in 1992 and 1994 and its scope expanded. Following three years of negotiation, at the OSCE Summit in Istanbul (1999), the *1999Vienna Document (VD99)* was adopted. Following the debates regarding the VD99 upgrade, within the special meeting of the Forum for Security Cooperation (FSC) on 30 November 2011, it was adopted the decision to republish the VD in the VD 2011 variant. VD 2011 includes the update decisions adopted between 2010- 2011, a total of 9 decisions having a technical nature. VD 2011 officially entered into force on 1 December 2011.

[14] Interview given by Margarita Simonyan, RT Chief Editor, 7 March 2013, cited by Heidi Reisinger, Aleksandr Golts, *op. cit.,* p. 7.

Also, another mission of Russian television was to prevent the damage of Russia's image, as it happened in 2008 in the five-day war in Georgia, when the media focused mainly on the damage caused by the Russian army.

All this was used to prepare the terrain for action in Crimea and Ukraine. The disinformation campaign included several components: systematic misinformation, labelling (labelling the Euromaidan movement as fascist), denial of apparent matters (such as involving the army in war), invoking humanitarian issues (sending convoys with humanitarian aid and requesting a corridor for refugees, and the soldiers of encircled Ukraine's), allegations of violations of international humanitarian law by the Ukrainian authorities (instigating the killing of Russian-speaking citizens), implementation of the Novorossiya concept (proclaiming on 24 May 2014 the independence of the *"New Russia"* state, including Donetsk, Luhansk, Dnipropetrovsk, Zaporizhia, Odessa, Mykolaiv, Kharkiv and Kherson).

ANALYSIS OF THE CHARACTERISTICS OF THE HYBRID CONFLICT IN THE CONCEPTION OF THE RUSSIAN FEDERATION

Summarizing, we can identify some features of the analysed conflict (Ukraine, 2014) in the present paper, from the perspective of hybridity, as follows:

- The conventional invasion component is replaced by an undercover force, concealed;
- The extensive use of political, economic, information, humanitarian and other non-military measures;
- Upsetting the local population;
- Transforming the population of the adversary state into a friend;
- The use of disguised armed forces;
- Cyber-attacks;
- Economic control actions;
- Purchase of political power;
- Speculation of corruption;
- Actions in the field of environmental protection;
- Insurgency triggered, fuelled and supported from outside the state under aggression;
- The induction of political instability;
- Precarious economic situation;
- Undermining the activity of the state government under aggression;
- Interstate conflict with the aspect of internal civil war;
- Destabilization of public life and state structures;
- Undeclared conflict;

- Replacing the conventional army with stateless, masked fighters;
- Activating/reactivating some separatist movements;
- Propaganda and imagological actions;
- Speculation of the demographic, ethnic and religious structure and the perception of public opinion;
- The organization of sophisticated military systems and training of insurgents/ separatists from outside;
- Internal and cross-border corruption;
- Making the most of the moment favourable to the outbreak of war;
- Psychological operations (PSYOPS);
- Incite violence;
- The Ukrainians tried to avoid the military confrontation with Russia, which annexed the Crimean Peninsula without facing opposition;
- The insurgency was concentrated in a particular part of the country;
- The civilian population was considered the centre of gravity.

CONCLUSIONS

From the analysis of the concepts of approaching the hybrid type conflict by the Russian Federation, we express the following opinions:

- as a rule, the Russian Federation considers that this type of conflict can be carried out in a permissive environment;
- for the Russian Federation, the permissive environment means the existence of areas that favour the actions of people of the same ethnic appurtenance, as well as of special forces that are accepted by the civilian population in support of separatist movements;
- in the context of hybrid conflicts, in the conception of the Russian Federation, the dominant forces and means are the irregular ones of insurgency type, ethnic separatism in combination with the unconventional ones of the type of special operations;
- regarding the appearance of military operations in hybrid conflicts, in the conception of the Russian Federation, the conflict is undeclared, the acting force is subversive and stateless, and the actions are carried out under the slogan of the consummated fact.

Given these conceptual aspects regarding the approach of hybrid conflicts, we appreciate that in the Russian Federation's vision the objectives to be achieved are to create enclaves for their control and to formulate requirements under threat and blackmail conditions.

BIBLIOGRAPHY

1. Mihaiu Mărgărit, Ucraina și războiul hibrid, în tentativele Rusiei expansioniste ale Moscovei de revenire a ei la masa marilor decizii ce privesc geopolitica mondială, in Pulsul geostrategic, no. 175, 20 September 2014, www.ingepo.ro.
2. Heidi Reisinger, Aleksandr Golts, *Russia's Hybrid Warfare – Waging War below the Radar of Traditional Collective Defence*, Research Paper, no. 105, November 2014.
3. Ana Stan, *Rusia a ridicat războiul la rang de artă*, 02.09.2014, adev.ro.
4. Igor Zevelev, *Russian National Security and Foreign Policy*, lecture delivered on 23 October 2014, *"George C. Marshall"* Centre for Security Studies, Garmisch-Partenkirchen, Germany.
5. Igor Zevelev, *The Russian World in Moscow's Strategy*, Center for Strategic & International Studies, see www.csis.org/analysis/russian-world-moscows-strategy.

INSTITUTIONAL ADAPTATION IN THE SECURITY ENVIRONMENT – A CASE STUDY ON THE CONCEPT OF SOCIAL NETWORK –

Dan MAZĂRE

PhD Candidate, "Mihai Viteazul" National Intelligence Academy, Bucharest

Current theorizations in military related studies outline the need for a fresh postmodern approach, extending the "modern", positivist foundation of military thought and aiming at increasing the potential of institutional adaptation, with both knowledge management and action related goals. Institutional adaptation gets a multi-level approach, extending from the frames used to conceptualize the space of military action, to the framework defined to set methodologies and procedures, down to the military action and its material related assets. In such a context, the "network" and the "social network" turned into pervasive concepts during the last two decades, defining a route to understanding the new increased complexity in the action space: for understanding the human terrain in military settings, the intelligence realm and its challenges, the law enforcement and the legal framework it is built on. A brief conceptual archaeology of the "network" term is employed to outline some peculiar transformations during the evolution of Romanian security institutions during the last decades, as parts and as an integrated ensemble, in terms of missions, values and operational approaches.

Keywords: military science, change management, social network, interoperability, social environment.

MILITARY SCIENCE AND INSTITUTIONAL ADAPTATION

Military science is an area of peculiar reflection, which has been in search of an identity for more than a century, in Romania and abroad, being both a result and a source of the transformations of the military institutions in the national state. Current attempts to (re)orient theorizing in the field of military studies add to the *"modern"*, positivist perspective a postmodernist dimension *("post")*[1], meant to increase the capacity of institutional adaptation in terms of military knowledge and action. Summarizing, the *"post"* orientation outlines a series of relationships between the objects and subjects of reflection in military and security related arenas, so that both determinism and the measurable uncertainty are regarded as limited and limitative, unable to provide support in approaching security's paradoxical situations (ethical, but also logical). We will not try to establish whether such a position is really a novelty, but the literature of military history seems to contradict both the innovative character and the possibility of a *"solution"*, in both Romania and the Anglophone world. Defining the *"problem"* – theme in a controllable framework is a precondition for any attempt aimed at identifying *"solutions"*, and the present paper advances in this direction by proposing an analysis focused on the concept of *"network"* and its avatars in the security environment: the usage of language mediates both modern and postmodern approaches of security and acts as the primary framework to convey meaning.

An incursion into the literature that accompanied the development of military science in Romania is able to highlight the way in which the field of military science has defined itself in direct relation with the evolution of the state and nation[2]. From the work of Nicolae Bălcescu in 1844[3], to the establishment of the first journal *România Militară (Military Romania)* in1864, from the debates that precede and follow the great conflagrations of the 20th century to the peacekeeping missions in the Balkans, Africa or the Middle East, from Dimitrie Gusti's ample research

[1] As example Chris Paparone, *The Sociology of Military Science. Prospects for Postinstitutional Military Design*, Bloomsbury Academic, 2013, Ben Zweibelson' articles from the *Small Wars Journal*, as well as *Design Theory and the Military's Understanding of Our Complex World*, published 08/07/2011.

[2] As an example, the work synthesis from the volume Victor Deaconu, Marian Niță (coordinators), *Elemente de sociologie* și *psihologie militară românească – Analiza ideilor militare românești dintre războiul de independență* și *al doilea război mondial*, Ediura Militară, București, 1988 or the more recent homage volume Alina Papoi, Adelaida-Mihaela Radu (eds.), *"România Militară" – Restituiri*, Editura Militară, București, 2014.

[3] Nicolae Bălcescu, *Puterea armată* și *arta militară de la* întemeierea *principatului Valahiei pînă acum*, Editura Academiei Republicii Populare Române, București, 1953 published in 1844 in the magazine *Propășirea*, editors: Mihail Kogălniceanu and Vasile Alecsandri.

and action programme, including *The Sociology of the Nation and the War*(1921) to theorizing securitization at the end of the 20th century, from the *"struggle of the whole people"* to the *"extended security"* concept, from the position war to the blitzkrieg, from propaganda to hybrid war, from the cavalry charge of the 8th Regiment – Călărași in the attack on Smardan on 12/24 January 1878, to the air raid of Dan Vizanty's squadron during the miraculous 10 June 1944[4] – reflecting on issues with relevance for the military field sought to reduce the distance between the practice and art or between the theory and science in military settings. And the dual character is perpetually found over decades and themes in distinctions such as experience-intuition, decision and choice – miracle, determinism – games of chance.

Browsing the archives of journals such as *Probleme de artă militară (Problems of Military Art* and *Gândirea militară românească (Romanian Military Thinking)*[5], mapping the conclusions of synthesis works that follow the development of specific military topics throughout decades and also the diversity and thematic complexity of volumes with unique themes, identifying topics that go in time as recurrent questions, the author of the present time is face to face with a perpetual evolution and transformation of the themes, concepts and facts investigated by what has been defined as military science. This evolution can be seen as a consequence of the lack of accumulation of knowledge in social sciences (tributaries of military science), as a perpetuation of violence and conflict, as a failure of the practice of post-conflict reconstruction, as an image of the ever-present arms race, as an inevitable expectation of surprise and betrayal in the intelligence activity, as always perfectible state of the legislative framework, as a supremacy of the Kafka processes at the expense of the primary meaning of bureaucracy and rationality, be it limited.

What does military science offer in such a context, beyond a space of socialization for professionals and amateurs, or impostors[6]? A place for a series of concepts hunted by other science fields or areas of professional activity, from war and peace to strategy and operation, from time to action to efficiency and effectiveness, from source of information to command and control. Whether we look at marketing, which discusses about guerrilla warfare or at business schools where strategies are debated, the analogies have as starting point the military field.

Any area of knowledge, whether scientific or philosophical, is defined by a set of concepts, between which an interweaving of meanings is formed, defining

[4] Daniel Focșa, *Dan Vizanty - Destinul unui pilot de vânătoare*, Editura Institutul European, 2010.

[5] In 1864, the journal *România Militară* is founded, but stopped later in 1866. In 1898, *România Militară* reappears as the official journal of the Defence Staff. From 1990, this has taken over the journal formula *Gândirea militară românească*.

[6] Norbert Wiener, *Intellectual Honesty and the Contemporary Scientist*, The American Behavioral Scientist, Vol. 8(3), 1964, pp. 15-18, intellectual honesty as an attempt to fight against personal beliefs, to include all relevant facts, evidences and reasoning, to quote contributors that have provided starting points and to not plagiarize.

and conditioning the ontology, epistemology and methodologies specific to the field: a framework of representation and understanding specific to the area of knowledge, whether we are talking about natural or socio-human sciences. Initiation in the field of knowledge involves covering these semantic – inter-conceptual paths, following the way in which concepts have evolved and have been used, in time and space. We will discover representative authors, series of succession in time, schools of thought extended both in space and in time. But beyond this conceptual archaeology, the concepts serve the positioning of the fundamental and particular questions that the area of knowledge, directly or indirectly, seeks to address. They define a theoretical-applicative ensemble that guides and allows the approximation of the physical phenomena in their development, both in natural sciences and in socio-human sciences.

In such a perspective, military science presents a number of peculiarities. Having its own semantic framework and generating a community around it, military science has evolved through interaction with other sciences, lacking its own epistemological or methodological apparatus, compensating through the space of experimentation – the laboratory as a space of victory and defeat in visible and invisible wars. It borrowed and used concepts and methodologies from socio-human sciences, seeking to draw distinctions between military art and science, between theory and practice.

SOCIAL NETWORK ANALYSIS – A SHORT CONCEPTUAL ARCHAEOLOGY

Part of a wider research project aimed at defining alternative scientific methods to be included in the portfolio of operational support activities of a national security institution, the present paper summarizes a series of observations on the particular case of *"social network analysis"*.

Thus, among the multitude of concepts that have been subject to debate in the military field of science, *"network"* has occupied a special place in the past two decades. Following the 9/11 events, *"network"* has received increasing attention in academic research programmes and become a pervasive topic of dialogue between the academia and the security institutions.

In other words, *"network"* has become a ubiquitous term, a concept frequently invoked in the public discourse on life and security at the beginning of the 21st century, *"went to war"*[7] in the global war on terror, but also in counter-insurgency operations and various theatres of operations, as a subject of analysis. Moreover,

[7] Paraphrasing the title of Eric Wakin's work, *Anthropology Goes to War: Professional Ethics & Counterinsurgency in Thailand*, University of Wisconsin, Center for Southeast Asian Studies, 1992.

the *"social network"* has added to the Internet a previously non-existent social level: in the context of developing *social media* in the virtual environment, interconnected computing machines allow the creation of environments in which digital resources are shared. Among these resources is the (digital) identity of the machines' users.

The Romanian word *rețea* is the adaptation of the Latin *retella*, designating a lot of interconnected entities. As for the English language and its *network*, etymology indicates the Roman construction techniques, *opus (work) retella (net)*. Its earliest confirmed usage came in the 16th[8] century, later being used to describe rivers, canals (in the middle of the 19th century), rail transport and electricity transport infrastructure (end of the 19th century) and radio infrastructure at the beginning of the 20th century.

Regarding the Romanian language, for the inter-war period, sources that explicitly use the term *network* have not been identified. Among the security institutions of the time, the term *agents ("agentura")* was preferred. Paradoxically, *network* would be identified in the vocabulary of Dimitrie Gusti's movement' representatives, initiated during the inter-war period with the purpose of understanding and *"transforming"* the Romanian society, and countryside.

Within the institutional framework and from a security perspective, with the change of the political regime in 1951, the term *network* began to be used to describe the institutionalized[9] modus of organization of the informants. However, unlike the *informants' network*, the anti-communist resistance is described in the official documents of the time by the term *gang ("bandă").*

Moreover, in 1952 a dedicated structure called Gangs' Service was set up within the General Directorate of State Security. This observation comes to exemplify the way in which the institutional framework responds to legislative changes, which in turn reflect the political transformations of the society. In the same context, one must understand the changes observed in the Romanian legislation regarding the definition of an organized criminal group.

The Penal Code (contained in Law 286/2009) defines in article 367 the organized criminal group as *"the structured group, consisting of three or more persons, constituted for a certain period of time with the purpose of committing one*

[8] Keith Briggs, *Etymology of the Words Network, Net, and Work*, http://keithbriggs.info/network.html, retrieved on 10 September 2019. A complementary perspective is provided by Umberto Eco in his work *From Tree to the Labyrinth. Historical Studies on the Sign and Interpretation,* Polirom, 2009, the network being approached as a distinct form of labyrinth, used in the encyclopedic organization of knowledge in the Illuminist period.

[9] *"The most important weapon held by the State Security in the fight against (...) is a well organized network of informants. – Normative prescription concerning the relationship with the informants –1951",* fragment quoted by Luminița Banu in *Utilizarea rețelei informative* în *reprimarea rezistenței armate anticomuniste*, http://www.cnsas.ro/documente/istoria_comunism/studii_articole/reteaua_informativa/Reteaua%20informativa.pdf., retrieved on 8 September 2019.

or more criminal offences in a coordinated manner". It is relevant to note that the current definition generalizes the definition previously proposed by Law 39/2003 by which the criminal group was defined as *"the structured group, consisting of three or more persons, which exists for a period of time and acts in a coordinated manner for the purpose of committing one or more serious offences, in order to obtain directly or indirectly a financial benefit or other material benefit; does not constitute an organized criminal group the group constituted occasionally for the purpose of committing one or more ad-hoc criminal offences and which does not have continuity, clearly determined structure or pre-determined roles for its members within the group".*

The change of definition certainly had consequences for the framing of charge brought before justice and for the workflow of some state institutions. The legislator's choice for the concept of group (*"structured"*) to the detriment of network is a research topic in itself, given that the common sense refers to the concept of network: from spokespersons of security institutions to the media, the term network is used predominantly. We notice that, when we look at the online environment, the possibility of creating a *"group"* is one of the services offered by the online *"network"* connection platforms, the *"group"* and the *"network"* being distinctly defined within the framework of these IT tools. These observations lead us to the attempt to distinguish between the conceptual objects used, group or network, and the discussion could be extended to formulas such as clan, band, ring etc.

In the early 2000s, in the context of the increasing visibility of social network analysis as an approach with potential institutional support, the social network analysis becomes an object of study for the academic community focused on small group theories. With a rich history, the study and theorizing of small groups continues to be a topic of interest for various disciplines[10], current approaches most often targeting a specific theme for organizational development (developing teams, developing training programmes). From the perspective of those who focus on small groups[11], the social network references the (small) group in two hypotheses: when we are dealing with that sub-structure of a network called clique, with the entities (nodes of the network) connected to each other , and when we deal with entity associations based on common values of the attributes that characterize them; in the latter, the social network analysis establishes the nature and specificity

[10] Richard Kettner-Polley, *A Brief History of Interdisciplinary Cooperation in the Study of Small Groups*, Small Group Research 47, no. 2 (2016), pp. 115-133.

[11] Nancy Katz, David Lazer, Holly Arrow, Noshir Contractor, *Network Theory and Small Groups*, Small group research 35, no. 3 (2004), pp. 307-332. Romanian sociology also provides significant contributions in the field through the work of Achim Mihu, in the second half of the past century; the micro-sociological model of analysis proposed by Mihu constitutes itself in a landmark for approaching small group theories.

of the exchange relations between the emerging groups of entities of the network. In other words, there are situations in which the generic character of the connections between the entities of a network can lead to the emergence of a group, seen in the sociological literature as an association in which individuals identify and interact based on common identity characteristics, having a sense of unity or joint action.

Referring to the literature that addresses legislative or public policy decisions for the management of organized crime, we will observe that *network* is defined by the specificity and structural characteristics of the interactions established between persons involved in carrying out illegal activities. It is from this point of view that in both USA[12] and Europe[13,] it has been regarded as an alternative to the hierarchical organization of the respective groups, supporting the decentralization and most of the times the internationalization of the activities.

This perspective generates a new question: is the social network a model, a simple abstract representation of the various forms of human associations (equally groups, clans or gangs, for example) realized by using the mathematical object called graph, or, on the contrary, is the network a concept that describes and/or explains the collective action within the society, having its own particularities?

If by social network we understand an alternative representation of an association of individuals (different from the hierarchical one), and having in mind the research objectives, we must emphasize the importance of using procedures and tools (information technology) that will lead to representation starting from available data.

We could say that such a model is able to detect, even if only through its graphic representation, useful information for addressing the respective association of individuals. If, on the other hand, through social network, we understand a particular form of association of individuals, a fundamental component of any form of social ontology, which mediates the transfer of individual (micro) action to the action of broader social categories (macro, at the extreme class, ethnicity, religion etc.), then we will seek to emphasize those particularities of the network that enhance communication, cooperation and mobilization beyond the visual representation.

The first option leads the intelligence officer towards a representation of the criminal group in a graphic form that highlights the relationships between the individuals, while the second option requires him to understand some topological and structural characteristics of the network, with consequences (causality)

[12] Jerome Bjelopera, Finklea Kristin, *Organized Crime: An Evolving Challenge for US Law Enforcement*, Congressional Research Service, January 2012.

[13] Paul A.C. Duijn, Peter P.H.M. Klerks, *Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement*, in *Networks and Network Analysis for Defence and Security*, pp. 121-159, Springer International Publishing, 2014.

in society, independently of individuals' characteristics. In the latter situation, we can observe how the information flow within the network and the mobilization of the individuals depends on the configuration of the network[14].

This pilgrimage in the social ontology aims to highlight the cyclical nature of the relationship between the main concepts used, group and network: within the group a network can manifest, within a network groups can appear, as a result of the relationships between the individuals who define the network. Three conclusions can be drawn from here:

a. Defining the social network as a potential abstract representation, a model, a social collective entity (group, clan, gang) based on the use of mathematical-informatic objects is required, but not sufficient;
b. Defining the social network as an entity in itself, which manifests and occupies a place in the social environment, supports the understanding of individual action feeding into collective action and equivalates the network with group, clan, gang ... a social collective entity which describes and explains causal relationships;
c. In current use of the term, we often omit this distinction, and using the term network places us, depending on the context, in one of the above-mentioned situations.

Although it may be considered trivial, the distinction previously made and the entire chain of argumentation aim to substantiate an observation that refers to the improper way of using indicators of social networks analysis. Thus, a software solution for analysing social networks encompasses into its functionalities algorithms with which we can easily calculate indicators of various networks (communications, financial, exchange, representing an organized crime group etc.). This does not mean that the results obtained and the values of the indicators can be interpreted in a similar way. Applying the same algorithm does not transfer the interpretation framework from one case to another, from one type of network to another.

In order to highlight the different frameworks for interpreting the results and the indicators, so that the social network analysis can become relevant in relation to the specificity of the network, we will consider the various theories regarding social networks, but also the practice of carrying out projects in which network analysis was used to address organized crime. Regarding the theoretical aspects addressed by sociology, Marian-Gabriel Hâncean[15] realizes an inventory of the theories, methodologies and current applications of the analysis of social networks, offering a starting point for this problem.

[14] Daniel Little, *New Directions in the Philosophy of Social Science*, Rowman Littlefield, Sep. 2016. chapter 3, *Social Things – What Exists in the Social Realm*, pp. 73-115.

[15] Marian-Gabriel Hâncean, *Rețele sociale – Teorie, metodologie* și *aplicații*, Polirom, 2014.

SOCIAL NETWORK ANALYSIS – SHORT CASE STUDY ON ORGANIZED CRIME LEGISLATION

In the past two decades, in the Romanian jurisprudence there have been debates on the doctrine and judicial practice that had as subject the organized crime. The debates focused on the articles of Law 39/2003, the old penal code – 1969 and the new penal code, which defined the organizational forms for committing crimes. The doctrine and the judicial practice were in an applied dialogue, reflected by the changes that have been made over the years of the legal framework that addresses this area of criminal law.

Romanian jurisprudence draws a distinction between occasional participation (author, co-author, instigator, accomplice) – criminal participation, seen as an occasional plurality and association – multiplicity in committing an offense, seen as a constituted plurality. Regarding the multiplicity, Law 39/2003 called for *"criminal groups"* (Art. 7, Art. 8) and the old penal code – 1969 explicitly referred to a generic form, *"the association for committing crimes"* (Art. 323).

In order for a person to be considered guilty for *"associating for committing crimes"* (Art. 323), as prescribed by the old penal code, it was not necessary for him/her to have been activated within the association or to know all the members of the group, it was sufficient to have expressed own will to be a part of the group constituted with a criminal purpose. The new penal code preserves the spirit of this approach, so that *"for the establishment of an organized criminal group"* (Art. 367, paragraph 1) it is stated: *"The initiation or the establishment of an organized criminal group, the accession or support, in any form, of such a group is punished with imprisonment from 1 to 5 years and the limitation on the exercise of certain rights"*.

From a legal perspective, when analysing the involvement in criminal activities, the social danger derives from the commission of the crime, the plurality defining an amplification of danger. The danger does not derive from the multiplicity of the perpetrators but only from the commission of the crime, the plurality being occasional. As for the associations for committing an offense, the social danger derives from the establishment and emergence of a multiplicity for committing several crimes. Thus, the association – the multiplicity has an independent existence, with a clear duration in time and implies an activity of planning and organizing criminal actions, the plurality being thus constituted.

In this conceptual-doctrinal context must the decision of the High Court of Cassation and Justice no. 12/2 June 2014 be understood. The subject upon which the High Court of Cassation and Justice ruled was to specify whether the new approach to the crime of establishing an organized criminal group, provided by art. 367 of the new penal code, discriminates or integrates the cases of plurality constituted

by offenders who do not take the form of an organized group, incriminated by art. 323 the old penal code or art. 8 of Law 39/2003.

The arguments state: *"as it follows from the explanatory memorandum of the new Criminal Code, the will of the legislator was to abandon the existing parallelism between the texts that incriminate this kind of facts (organized criminal group, association for the commission of crimes, plot, terrorist grouping), before its entry into force, in favour of establishing a general incriminatory framework – the establishment of an organized criminal group – with the possibility of maintaining as a distinct crime the establishment of terrorist association, given its specificity"*[16], as it is also apparent from the Court's decision 823 / 12.12.2017 Constitutional, regarding the exception of unconstitutionality of the provisions of art. 367 para. (6) of the Penal Code[17].

The present article seeks to identify those contexts in which the term network was used in the last decade in the specific argumentation of various criminal cases in Romania. Thus, information from a database integrating national sentences given between 2007 and 2018, accessed via the online platform sintact.ro was analysed from a qualitative perspective.

This exercise follows at the level of intention the debate that animated the Dutch society[18] in the mid-1990s, when in an inter-institutional format the legal perspective on organized crime was redefined.

In the Romanian case, the network is an implicit term used in arguing the structured character of the crime; the explicit references to this term are missing in the official legislative documents. The doctrinal dialogue is also reduced at the level of the legal universe, lacking the inter-institutional character in defining this issue. As a consequence, the inter-institutional protocols established are difficult to evaluate not only from the point of view of their effectiveness and efficiency but above all, undocumented and questionable in meaning and purpose.

The analysis drew some conclusions, as follows:

If the object of the analysed sentences is the human trafficking/minors/ migrants/ drugs, the term network is predominantly used to describe the facts. Furthermore, in most situations, the defence invokes the fluid character of the network as an argument for reducing the sentence:

Criminal sentence no ___ / 2014 of 24.11.2014, Timiș Court

"... as he showed before the first judicial instance and before the court of appeal, his only contacts with this network (of traffickers) were when he contacted AT

[16] Decision no. 393/ 28 May 2015, published in the Official Monitor of Romania, Part I, no. 609/ 12 August 3015, para 33 and 34.

[17] *Ibidem.*

[18] H. G. Van de Bunt, *Organised Crime Policies in the Netherlands*, in Cyrille Fijnaut and Letizia Paoli (eds.) *Organised Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond*, Springer, 2004, pp. 677-716.

*for a supply of drugs and that, as declared by the accused AP, the **man did not even know him, nor the rest of the network's members or its extent**";*

Sentence no ___/2014 of 23.07.2014, Timișoara Court of Appeal

*"... the accused requested a review of his sentence, given that he had a marginal involvement in the criminal activity, being a drug user that accepted to participate in the transport of a quantity of drugs, **without having any contribution** to the purchase of these drugs or **in establishing links with persons in the network** or to identify possible clients".*

If the criminal sentence was given on *"the association for committing crimes"*, the network is also the default term used to define the association. Most of the time this is regarded as being organized around a person:

Criminal sentence no ___/2015 of 11.09.2015, Galați Court

*"... during 2001 - September 2002 the defendant CRF was part of a criminal association constituted for the purpose of committing crimes of human trafficking, trafficking of minors and pandering, **coordinated b**y the perpetrator NM ... the deed of the defendant meets the constituent elements of the association offense for the purpose of committing crimes provided for in article 323 paragraph 1 Criminal Code";*

Criminal sentence no ___/2013 of 31.01.2013, Pitești Court of Appeal

*"... **The coordinator of this network** and the one who, in fact, had the most significant contribution to committing human trafficking was the defendant ZI. According to the files, he recruited women with fictitious promises of marriage, after which he forced them to prostitute";*

Criminal sentence no ____/2011 of 27.12.2011, District Court 4 Bucharest

*"... It is true that for the criminal association to exist and act in a criminal manner, it is not necessary for all members of the group to know the role played by the other members. It is not possible to assign him the position of leader of the criminal grouping only because in many cases he would have asked the defendant GA to pay a certain debt that he had, especially **that as a leader**, this defendant should have known in detail what the offenses to be committed will consist of, the modus operandi and the roles of each defendant ... ".*

If the criminal sentence concerned *"the establishment of an organized criminal group"*, the term network is also used **in describing** the structuring process:

Conclusion no ___/2015 of 17.03.2015, Bucharest Court of Appeal

"... The Court finds that in the case subjected to examination, the conditions stipulated by the legislator regarding the existence of the organized criminal group are met, as the group has as initiator and leader the defendant IP, as well as

*continuity, a determined structure, predetermined roles, a hierarchy in which two levels are clearly highlighted, decisional and executional ... and from the evidence provided in the case it resulted that the defendants ... knew the criminal activity of each member of the group, having **the representation of an illicit network** of prostitution in Romania and abroad, collaborating in criminal matters";*

Decision no ____/2015 of 10.11.2015, Bacău Court

*The criminal investigations carried out in this case have identified as members of the criminal group the following persons ... that **established a real network of distribution** of cigarettes obtained through smuggling, structured on several levels (cells), according to their roles in within the group. The defendants were located on **the upper level of decision** within the group. They live within the boundaries of the border counties ... and had the role of collecting cigarettes that were illegally introduced into Romania by unidentified persons, in order to market them through the defendants located at the lower levels of the group. On **the second level of the group** were the defendants ... **who acted as intermediaries**.*

In the before mentioned cases, the *network* is seen as a common good, useful, invoked to support the referral to a certain legal provision, and to highlight the structured character of the criminal organization, in a constituted plurality. We note, however, the side effects of this ad-hoc use of the term, in the absence of clear legislative provisions: the use of the fluid nature of the network to request the review of the sentence and the frequent attribution of both an eminently hierarchical and centralized structure to a criminal organization, and a decentralized, network-specific perspective. In such a context, the network becomes a mere stylistic element in the argument: if the network is ubiquitous, it becomes absent.

CONCLUSIONS

Ensuring the security of the contemporary nation state continues to be mainly perceived as an institutional process, having been granted specific implementation mechanisms (institutional-functional) to cover the sovereignty and independence of the state. In the military and law enforcement agencies, but also within the institutions that provide the information support for security decision, such as intelligence organizations, the operating paradigm is monolithic, bureaucratic, reflecting a realistic ontological approach, in which entities and processes are empirically perceived in rationalist logic (action and purpose, causality entity – process and means – objectives, measurement and adjustment, action in order to reach a desirable *"final state"*).

Military science does not propose an epistemological, ontological and methodological apparatus specific to the field, and multi- and interdisciplinarity cannot be placed in a well-defined frame of reference. However, through the extensive literature

in the field we have access to a large number of analyses on current issues. In such a context, indexing and organizing knowledge in the form of journals or periodicals is a prerequisite for developing and maintaining an identity of military science.

The conceptual outline of the term *"network"*, as understood and used in Romania, highlights the possibility of opening a new path of research and accumulation of knowledge, namely the development of a conceptual history of security and intelligence in Romania. Such an approach can reveal *"who are"* those who operate in military science, as a distinct social body, starting from the history of the language used in the security environment, to the vocabulary of the security.

A brief case study reveals the paradoxical situation regarding the use of the concept of *network* in the legal environment. Although we note the absence of a clear definition in legislative documents, and the lack of contexts suitable for the use of the concept in judiciary activities, *network* is used in formal settings without a sound basis. The media also uses this term to present forms of organized crime, preferring it over the legally accepted formulas.

From this perspective, understanding social network analysis constitutes itself in a pertinent example to initiate a dialogue between security and intelligence institutions and the Legislator, for defining a sustainable mechanism for legislative change. Furthermore, this example seeks to emphasize the understanding of the interaction between military science and social science in Romania. In the hectic context that affected the higher education environment, understanding the need to relate to the cultural-scientific history, both in the military and social sciences, was and remains an imperative, just like any other systemic construction initiative.

In this overall framework, the attempt to establish the place and role of the social network analysis as operational support mechanism in security and/or intelligence organizations becomes a generic, complex and complete problem. Solving such a problem and identifying proper ways and stages of adopting it as a work methodology allows for the security institution to clearly define means to replicate the process in other situations in which social science can provide added operational value. Thus, we are dealing with a problem whose solution offers arguments to establish an institutional adaptation framework that combines both pragmatism and metaphysics, realism-positivism and postmodernism or post-institutionalism, as defined in this decade, in relation to the assumed mission of military national organizations. The usage of language mediates both modern and postmodern approaches of security and acts as the primary framework to convey meaning.

BIBLIOGRAPHY

1. ***, *Decision no. 393* on 28 May 2015, published in the *Official Gazette of Romania*, Part I, no. 609 on 12 August 2015, para. 33 and 34.

2. Luminița Banu, *Utilizarea rețelei informative* în *reprimarea rezistenței armate anticomuniste*, http://www.cnsas.ro/documente/istoria_comunism/studii_articole/reteaua_informativa/Reteaua%20informativa.pdf.
3. Nicolae Bălcesu*, Puterea armată* și *arta militară de la* întemeierea *principatului Valahiei pînă acum*, Editura Academiei Republicii Populare Române, București, 1953.
4. Jerome Bjelopera, Kristin Finklea, *Organized Crime: An Evolving Challenge for US Law Enforcement*, *Congressional Research Service*, January 2012.
5. Keith Briggs, *Etymology of the Words Network, Net, and Work*, http://keithbriggs.info/network.html.
6. H. G. Van de Bunt, *Organised Crime Policies in the Netherlands*, in Cyrille Fijnaut, Letizia Paoli (eds.) *Organised Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond*, Springer, 2004.
7. Victor Deaconu, Marian Niță (coordinators), *Elemente de sociologie* și *psihologie militară românească – Analiza ideilor militare românești dintre războiul de independență* și *al doilea război mondial*, Editura Militară, București, 1988.
8. Paul A.C. Duijn, Peter P.H.M. Klerks, *Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement*, in *Networks and Network Analysis for Defence and Security*, Springer International Publishing, 2014.
9. Umberto Eco, *De la arbore spre labirint. Studii istorice despre semn* și *interpretare*, Polirom, 2009.
10. Daniel Focșa, *Dan Vizanty - Destinul unui pilot de vânătoare*, Editura Institutul European, 2010.
11. Marian-Gabriel Hâncean, *Rețele sociale – Teorie, metodologie* și *aplicații*, Polirom, 2014.
12. Nancy Katz, David Lazer, Holly Arrow, Noshir Contractor, *Network Theory and Small Groups*, *Small Group Research* 35, no. 3, 2004.
13. Richard Kettner-Polley, *A Brief History of Interdisciplinary Cooperation in the Study of Small Groups*, *Small Group Research* 47, no. 2, 2016.
14. Daniel Little, *New Directions in the Philosophy of Social Science*, Rowman Littlefield, September 2016.
15. Chris Paparone*, The Sociology of Military Science. Prospects for Postinstitutional Military Design*, Bloomsbury Academic, 2013.
16. Alina Papoi, Adelaida-Mihaela Radu (eds.), *"România Militară" – Restituiri*, Editura Militară, București, 2014.
17. Eric Wakin, *Anthropology Goes to War: Professional Ethics & Counterinsurgency in Thailand*, University of Wisconsin, Centre for Southeast Asian Studies, 1992.
18. N. Wiener, *Intellectual Honesty and the Contemporary Scientist*, *The American Behavioral Scientist*, Vol. 8(3), 1964.
19. Ben Zweibelson, *Small Wars Journal*, *Design Theory and the Military's Understanding of Our Complex World*, published on 08/07/2011.

DYNAMICS AND TRANSATLANTIC COOPERATION IN THE FIELD OF ENERGY SECURITY

Ioan MANCI, PhD
Lecturer, "Babeș-Bolyai" University, Cluj-Napoca

Mihai Ionuț RUSU
PhD Candidate, "Babeș-Bolyai" University, Cluj-Napoca

Energy, in the context of the current economic, social and geopolitical dynamics, continues to be one of the topics of great interest for all the political and military actors in the international relations scene. In this paradigm, the cooperation of key actors, such as the European Union and NATO, is essential, given that energy security is a strategic element of great interest and interconnectivity in their acceptance. The economic, geopolitical challenges, as well as the impact of the current climate change to which the international environment is subject, make the member states of these organizations directly involved and responsible both in relation to the other international actors and in terms of the security of their citizens. The dynamics of the security of the European and transatlantic energy sector is intensifying as actors use energy resources as coercive elements. Instead, humanity faces the realities of the effects of climate change, and geopolitical conflicts threaten the development and sustainable existence of states.

Keywords: energy security, resources, climate change, NATO, European Union.

GENERAL ASPECTS REGARDING ENERGY SECURITY

This analysis aims to provide a current overview of the contemporary international landscape of energy security, which is continuously dynamic on both sides of the Atlantic. Currently, through energy security we can identify the economic, political and military capacity of a country to maintain its vital national interests and the availability of the energy resources needed to perform this fundamental function.

Therefore, for a national or international actor who enjoys a high degree of security, the energy flow will be uninterrupted and accessible. The concept includes much broader considerations, such as environmental sustainability and the ability of the energy system to respond flexibly to sudden imbalances between energy supply and demand. Also, due to traditional security considerations, it is necessary to carry out an assessment of the strength of the energy system as a whole, in the face of a possible attack through direct military operations or emerging forms of asymmetric offensive operations.

The transatlantic community has made significant progress in using global energy resources to ensure energy security, due to technological advances in the field of renewable energy, energy efficiency, the discovery of new deposits, the development of alternative sources and routes, but also of new infrastructure. However, security challenges for European energy continue to emerge as state actors use energy as a form of geopolitical repression, thus threatening security of supply and sustainable development of society, all the while the international communities facing the negative effects of climate change.

Transatlantic energy security cooperation is essential to addressing these global challenges and should be a priority of the USA, the European Union and NATO, as energy security can be translated automatically into national, economic and social security.

Assessing the progress made towards liberalizing and integrating European energy markets requires an imperative identification of the US commitment to EU energy security. Commitment that will be more effective and will be able to explore the obstacles to the efficient functioning of energy markets and highlight priorities for USA-EU cooperation.

In the conditions of increasing the degree of complexity of today's globalized world, the increased level of interdependence and the drastic diminution of the energy resources, in the context of the increase, most often uncontrolled,

of the consumption at international level, the major challenge of the nations and the politico-military organizations consists in increasing the level of uncertainty regarding the energy security of the states and their citizens.

If the European Union remains united and strong it will be much more resistant to energy challenges, and the United States of America will have the opportunity to have a strong ally, with vast investment opportunities in the energy field. US engagement in European energy security is driven by member states' strategic priorities, mutual economic interests and transatlantic interests in liberalized and integrated energy markets. Also, involvement in European energy security creates the opportunity to reinvigorate transatlantic links in times of uncertainty and national transformation in the energy sector.

ENERGY SECURITY FROM THE PERSPECTIVE OF THE EUROPEAN UNION

The general picture of the current energy mix of the European Union demonstrates the diversified need for energy sources, but also the crucial role that imports play in meeting energy needs. The European Union faces various challenges, including a strong dependence on imported fossil fuels (coal, natural gas, oil). In contrast, domestic fossil fuel production is declining across the EU, either due to limited reserves and environmental issues, or due to commercial considerations. In recent years, the main elements of the EU energy mix are represented by renewable resources and natural gas, reducing the share of solid fuels and petroleum products.

The EU legislative framework on energy security focuses on the natural gas and electricity markets, reflecting the particular cross-border challenges associated with security in this energy sector.

The energy policies developed by the European Union are governed by several concepts, but we can recall here three of the most important objectives[1]:

- reliable energy sources that provide, at any time and at any place, the necessary energy supplies;
- ensuring that energy providers operate in a competitive environment and will establish affordable prices for homes, businesses and industries;
- the energy consumed is sustainable, by reducing the emissions of greenhouse gases, pollution and dependence on fossil fuels.

If these goals are given particular importance and the path of the measures and interests that are required will be respected, the EU will be able to create a stable and favourable energy security climate, as this organization is one of the largest consumers of energy resources globally.

[1] Sanam S Haghighi, *Energy Security - The External Legal Relations of the European Union with Major Oil and Gas Supplying Countries*, Oxford and Portland, Oregon, 2007, p. 3.

The goal of a resilient energy union, with an ambitious policy and the influence of climate change at the centre, is to provide residential or industrial consumers with a safe, sustainable, competitive and affordable energy. Achieving this objective will require a fundamental transformation of the European energy system.

For example, the *Energy Union Strategy* has set more goals. The focus is both on the proper functioning of the single market and on the promotion of renewable sources and energy efficiency schemes that improve energy security by reducing dependence on imported fossil fuels. Launched in 2015, the *Energy Union Strategy* of the European Union is a five-year strategy that mandates EU countries to develop national energy and climate change plans. It covers five dimensions, namely: security, solidarity and trust; a fully integrated internal energy market; energetic efficiency; decarbonisation of the economy; and research, technology and innovation[2].

The European vision is identified with that of an energy union in which the member states know that they are interdependent with regard to the security of energy supply of their citizens, on the basis of real trust and solidarity, as well as of an energy union that expresses itself in unity worldwide.

The robust evolution of the development of renewable energy and the massive investments in energy efficiency will be able to cover the necessary capacity of these actors. However, natural gas and liquefied natural gas pipelines will be able to play a vital role in fuelling Europe, as the fuel undergoes a transition process, thus bringing about economic and energy change, while also reducing the level of carbon emissions.

The EU also has an essential role to play in improving energy efficiency and savings in promoting the use of renewable energy sources[3]. This can have a positive impact on energy security, as renewable energy is more likely to be produced domestically than fossil fuels. The latter are mostly imported from third countries. Measures to reduce energy consumption can further reduce energy imports and improve security of supply.

The dependence on energy imports is expected to increase[4] as coal and nuclear resources will diminish, and with it, the rest of domestic energy production will continue to decline. Thus, the transport sector is accelerating electrification and EU Member States are developing plans to meet climate goals under both the Paris

[2] European Commission, *Priority: Energy Union and Climate,*https://ec.europa.eu/commission/priorities/energy-union-and-climate_en, retrieved on 28.08.2019.

[3] Article 194 of the Treaty on the Functioning of the European Union 2012/C326/01.

[4] European Report from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions Energy prices and costs in Europe SWD (2019) 1 final, Brussels, 2019.

Agreement and the *Energy Union Framework Policy*[5].

The new rules require EU countries to work together in regional groups to assess the risks of supply disruption and to agree on joint regional actions. To address these risks, the Union has introduced a new *"solidarity principle"* that requires countries to prioritize helping neighbouring countries to provide vulnerable consumers in times of crisis[6]. Natural gas operators are now required to notify national authorities of major long-term supply contracts that could affect security and supply.

Notable are regional efforts, such as the *Three Seas Initiative*, led at the presidential level by twelve countries between the Baltic, Adriatic and Black Seas, which could greatly benefit from closer engagement with the EU and USA involvement in strategic infrastructure from Central and Eastern Europe. The *"Three Seas"* initiative aims to improve connectivity in energy networks, transport and the digital environment through coordinated regional financing mechanisms, such as the *Three Seas Investment Fund*.

Energy is a global challenge that nevertheless has strong regional characteristics. With regard to the energy sector, the biggest challenge is the need to upgrade the network to cover an increased share of renewable energy sources and local energy generation on national markets, but also with increasing cross-border capacity.

European energy leaders recognize natural gas as *"an important component"* of the EU's energy mix, but its role will evolve by the middle of the century to become a *"complement"* to the generation of electricity from renewable sources[7]. About one quarter of all energy used in the EU is composed of natural gas, where this paradigm has made natural gas a priority area for EU security actions. Many EU member countries are sourcing from outside the EU, and some states are largely dependent on a single source or a transport route. Interruptions that may occur along this route may be caused by vulnerable infrastructure failures or political disputes, which may endanger energy stability.

The European institutions have reached multiple resolutions such as: an agreement on the review of the regulation of natural gas imports, an updated regulation on the security of electricity supply, revised intergovernmental agreements in the energy field, natural gas-oriented directives and the application of its key provisions for pipelines with third countries. Also, new targets for energy efficiency and investments in renewable energy have been set with a view to 2030.

[5] European Commission, *Priority: Energy Union and Climate*, https://ec.europa.eu/commission/priorities/energy-union-and-climate_en, retrieved on 27.08.2019.

[6] European Commission, *Securing Europe's Gas Supply: New Regulation Comes into Force*, https://ec.europa.eu/info/news/securing-europes-gas-supply-new-regulation-comes-force-2017-oct-27_en, retrieved on 27.08.2019.

[7] Frederic Simon, *Cañete Sees Gas as "a Bridge" to Reach EU's Clean Energy Goals*, Euractiv, 2019, https://www.euractiv.com/section/climate-strategy-2050/news/canete-sees-gas-as-a-bridge-to-reach-eus-clean-energy-goals/, retrieved on 30.08.2019.

Parliament adopted several resolutions on its own initiative in the field of energy, including the EU Strategy for the storage of liquefied gas and natural gas[8], which is essential for the security of natural gas supply. EU projects of common interest are important drivers in financing energy infrastructure to improve interconnections and support security of supply.

Ensuring sustainable energy resources requires ongoing efforts from the EU and the Member States, involving vigilance over the reliability of third-country suppliers, assessing how new supply routes (or shutting down old ones) can affect energy security. Verifying that energy agreements with third countries are in line with EU objectives, it is confirmed that national energy choices do not adversely affect security of supply at regional level.

European energy must be maintained throughout this delicate energy transition, away from fossil fuels and oriented towards renewable sources. In addition, some key renewable energy sources have a variable supply that is not fully predictable. This is why it is vital for EU national authorities to properly coordinate their energy policies in order to avoid sudden increases or losses. The Union will maintain a key role in monitoring the security of supply throughout the energy transition from the old centralized generation system, dominated by fossil fuels on national markets, to a new system characterized by a high share of renewable sources, localized and cross-border production.

A positive development of EU energy security is the fact that it is actively resorting to reducing energy consumption and growing economies, as well as promoting and stimulating the use of renewable energy sources, which have a positive impact on energy resilience by reducing dependence on imported fossil fuels. Many renewable energy sources are locally generated (wind, solar, hydro, biomass) or supplied regionally, if such production is commercially stimulated or viable (biofuels).

Significant progress can be noted in mitigating threats from suppliers through significant investments in infrastructure, development of alternative gas routes and improvement of the regulatory framework. However, the emphasis must fall on the promptness of identifying and countering symmetrical and asymmetrical threats to the European energy network.

Access to a well-integrated internal pipeline network remains essential for European energy security, as gaseous fuels represent 23% of the EU's total energy needs, being second in oil, with about 36% of the total energy mix[9]. Gas is not as fungible as oil, which means it is not as easy to market in global markets.

[8] EU strategy for liquefied natural gas and gas storage, European Parliament resolution of 25 October 2016 on an EU strategy for liquefied natural gas and gas storage (2016/2059 (INI)).

[9] European Commission, *In-depth Study of European Energy Security,*https://ec.europa.eu/energy/sites/ener/files/documents/20140528_energy_security_study_0.pdf, retrieved on 23.08.2019.

European gas markets have become much more liberalized and connected, and price discrepancies in EU countries and regions are evidence of infrastructure bottlenecks and market distortions caused by a single dominant supplier.

The issue of energy security has become a diplomatic vector within the European Union. This is especially accentuated by the conflicts between Russia and Ukraine when, in the winter periods between 2006 and 2009, Russia temporarily stopped natural gas trade to European consumers, causing serious supply problems in some EU countries.

Following the annexation of Crimea, the Russian Federation intensified its political conflicts in Ukraine, and the EU tested the energy sectors in EU Member States through neighbouring countries. These challenges focused on analysing the ability of EU countries to withstand emergencies in energy supply. The direct result of the tests was a revision of the Regulation on the security of gas supply, and the revision entered into force in 2017[10]. Russia still holds the largest reserves of natural gas in the world, more specifically 25.02% of the world's proven natural gas reserves on the planet[11], currently being Europe's main energy provider, a trend that continues even in the near future.

The economic and geopolitical situation in 2014 led to the existence of a single major natural gas supplier for Europe. The new socio-economic paradigms created diplomatic and economic tensions that indirectly affected the West, by stopping the supply of natural gas. To ease the situation, the European Commission was actively involved in the negotiations that lasted several months, and the solution was to sign an agreement that led to the resumption of energy supply. The European Commission has thus made significant progress in achieving the regulatory objectives of the Energy Union.

Another significant uncertainty is the impact of Brexit on EU energy markets in the short and medium term. An external study conducted for the ITRE committee in 2017[12] suggested that the impact of Brexit on the energy system on EU citizens and companies should be limited, but argued that particular attention should be paid to its impact on the Irish energy system.

Economic and geopolitical forces are converging, as Europe gives priority to future energy investments in European countries that are facing the need to finance infrastructures essential for energy security. Substantial EU support

[10] European Commission, *Securing Europe's Gas Supply: New Regulation Comes into Force*, 2017, https://ec.europa.eu/info/news/securing-europes-gas-supply-new-regulation-comes-force-2017-oct-27_en., retrieved on 23.08.2019.

[11] Alexander Mercouris, *Russia Wins Energy War in Europe after EU Surrenders on Nord Stream 2*, in http://theduran.com/russia-wins-battle-eu-nord-stream-2/, retrieved on 25.08.2019.

[12] European Parliament, *The Impact of Brexit on the EU Energy System,* https://www.europarl.europa.eu/RegData/etudes/STUD/2017/614181/IPOL_STU(2017)614181_EN.pdf, retrieved on 25.08.2019.

for such projects has been essential for upgrading and alternative options for energy supply, providing only benefits for energy security.

The European Union must be constantly vigilant in monitoring energy markets, ensuring that as these energy markets change, energy security for residential, business and social services is maintained at all times.

ENERGY SECURITY VISION OF THE UNITED STATES OF AMERICA

Energy security remains a priority issue for the United States of America. The country continues to demonstrate a strong focus on reliability and resilience, recognizing that its national and economic security depends on the reliable functioning of its energy infrastructure. The government has taken steps to update its security frameworks, including by introducing processes that address new trends, such as asymmetric threats. US energy exports are already playing an important role in diversifying global energy supplies and mitigating the potential impact of disruption events.

The shale gas revolution will turn the United States of America from a net energy importer into a net exporter by 2020, as increased production of crude oil, natural gas and liquefied natural gas exceeds consumption. As the United States of America is able to further increase production over the next decade, facilitating the construction of support infrastructure will be a key factor in maximizing the benefits of shale gas, both internally and externally. This revolution has made the United States of America not only the world's largest producer of oil and gas, but also a major exporter.

The approach to the process of developing energy policies has shifted from a mentality that focuses on energy security to one that seeks to maximize the benefits of energy. To this end, the current policy of the US government focuses on the concept of *"energy dominance"*, which reflects a strategy for maximizing energy production, benefiting from higher energy exports, being a global leader in energy technologies and maintaining the energy bills of the consumers[13].

The United States of America has encouraged the energy revolution generated by shale gas discovery and exploitation[14]. As a result, global liquefied natural gas markets have focused on pricing mechanisms based on this market. Technological improvements such as hydraulic fracturing and horizontal drilling have led to the development of unconventional natural gas resources, such as shales and other rocks

[13] International Energy Agency, *Energy Policies of International Energy Agencies Countries: United States 2019 Review,* 2019.

[14] Ellen Scholl, *The Future of Shale: The US Story and Its Implications*, https://www.atlanticcouncil.org/publications/reports/the-future-of-shale, Atlantic Council, 2019, retrieved on 10.10.2019.

with lower permeability[15]. Improved efficiency has reduced production costs, making shale gas economically competitive at almost any price and allowing large-scale exports.

The price of natural gas is moving away from the prices of oil-related products and is oriented towards hybrid, market-based, and on-the-spot prices. The *"take over or pay"* and *"destination"* clauses in contracts – which restrict gas transportation and unloading locations that prevent buyers from selling excess merchandise – are becoming less popular and, in some cases, outdated[16].

The United States of America has an important role to play as a reliable supplier for Europe, and the transatlantic allies have a unique opportunity to work together to manage key trends in the natural gas market, leading to a shift towards more liquidity, transparency and global competition. Another important objective is for Europe to establish a competitive market, where supply can come from many sources, including the United States of America, Qatar, Algeria, Australia and elsewhere.

Energy security can also be regulated through certain key tools of this industry. For effective engagement with the European Union, on future progress in the energy sector, the United States of America needs to understand and recognize more European legislative improvements, technological advances and the need for cooperation in this area.

Greater involvement of energy consumers would have a significant impact on the natural gas market. Energy consumers are engaged in the details of where their energy comes from, how it is used and what impact different sources have on the environment. Education, open dialogue, transparency and strengthening relationships with communities are essential for the successful development of energy projects. Some European constituents face American interests with difficulty due to environmental and climate issues. It is important for the EU to have a consistent communication on the role that natural gas will play in fulfilling the environmental stages of the Energy Union.

To help this end, the United States of America and the EU could work more closely in public communication and develop a transatlantic strategy to educate consumers on the geopolitical and energy security benefits of energy infrastructure projects. These include wind turbines, transmission lines and natural gas infrastructure, as well as clear messages about the impact of hydraulic fracturing practices on the environment.

[15] Federal Energy Regulatory Commission, *Energy Primer: A Handbook of Energy Market Basics*, 2015, p. 10.

[16] Aaron Sheldrick, *Destination Clauses on LNG Will Soon Fade Away: Gas Union President*, https://www.reuters.com/article/us-asia-lng-contracts/destination-clauses-on-lng-will-soon-fade-away-gas-union-president-idUSKBN0LT0YY20150225, Reuters, 2015, retrieved on 28.09.2019.

Supporting strategic energy infrastructure is essential for security projects, but it may take several years to become economically viable. A common strategy would allow the EU and the US to eliminate threats and identify common strategic priorities, providing a stronger front against competition or negative influence from global players whose investments could pose energy security risks.

Investment opportunities would ensure consistency and support for the priorities of existing primary forums for EU-US dialogues in the fields of digital, transport and energy. This signals a new era of US strategic investment and foreign aid, assuming a greater focus on mobilizing private investments.

To be proactive in providing solutions for the threats to transatlantic energy security as well as for the necessity to connect infrastructure, the USA and EU need a comprehensive strategy regarding the relations with Russia, China, and the geopolitical points of interest such as the eastern Mediterranean Sea and Ukraine. The energy sanctions imposed on Russia by the USA could have an important impact on the transatlantic relations[17]. Even when sanctions do not explicitly target the EU, the indirect consequences of sanctions can adversely affect EU businesses, including through secondary sanctions.

Uncertainty about sanctions against Nord Stream 2 was one of the factors that contributed to the necessary pressure on the USA European allies to address Russian monopoly behaviour, by rapidly passing the amendment to the Gas Directive[18]. US sanctions may still be valid as a deterrent.

Close engagement and transatlantic coordination are essential in trying to avoid the negative consequences for US allies. Transatlantic unity is essential to ensure political and economic pressure on actors who attempt various types of geostrategic constraints.

Analysing the achievements and opportunities of infrastructure regulation has exposed several areas that could benefit from more proactive transatlantic cooperation, including sustainable and coordinated financing mechanisms on energy markets that provide a level playing field for suppliers. It is also worthwhile to take stock of current US commitments in these issues to identify an effective path.

NATO AND ENERGY SECURITY

NATO's role in building transatlantic energy security has been the subject of discussion and debate in recent years. Energy security is to a large extent a problem of structuring energy markets than of defence. The existence of other institutions, besides military ones, must be recorded.

[17] US Department of the Treasury, *Countering America's Adversaries through Sanctions Act*, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/caatsa.aspx, retrieved on 28.09.2019.

[18] US Department of Energy, *US-EU Energy Council,* https://www.energy.gov/ia/international-affairs-initiatives/us-eu-energy-council, 2019, retrieved on 30.08.2019.

NATO has a significant dependence on civil and commercial infrastructure, including military transport, communications used for defence purposes and supporting national services for NATO operations in infrastructure and local commercial services. Many of these dependencies do not have low availability[19], raising the need to identify and generate failure points potentially vulnerable to exploitation through hybrid interference and influence.

Energy is a strategic and vital asset for the operation of military forces. Therefore, military geostrategies must ensure that the companies they defend have access to this strategic asset and, of course, that their armies are functional. From these considerations we can say that the defence of critical infrastructures is part of NATO's competence to ensure security. Security has become even more difficult, with the development of other asymmetrical and less conventional war techniques. Threats to these infrastructures are diverse and can be issued not only by state actors, but also by other international or national actors.

The emergence of asymmetrical attacks on vital energy assets has increased in recent years, which has led to increased defence capabilities for strengthening these assets. NATO can be an important landmark for the exchange of information impacting this area, but also for best practices to reduce the risks of such attacks and to meet these challenges. Also, within the organization there is an exchange of experiences and information between its members on various energy security issues, such as fierce competition in the resource market, climate change and how they shape a broader security framework.

In view of energy efficiency, the North Atlantic Alliance has made sustained efforts to reduce the energy costs of its forces while increasing the awareness of the military environment, shared with all its members and allies.

The Alliance works with other international bodies to increase their own situational awareness. In this regard, another important international body is the International Energy Agency, which has enormous responsibilities in formulating international efforts to strengthen energy security. This has become a solution for sharing information on energy issues and their links to security.

As many NATO allies depend on Russian gas and oil, the resilience of energy infrastructure plays a particularly important role in crisis situations, in the common security of NATO member states. Therefore, identifying stable and reliable energy sources, diversifying transport routes, establishing suppliers and energy resources, and understanding the interdependencies of energy networks are of vital importance for increasing the resistance against hybrid threats[20]. In this regard, improving

[19] NATO, *Resilience and Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, retrieved on 29.08.2019.

[20] NATO Energy Security Centre of Excellence (NATO ENSEC COE), *Energy Security: Operational Highlights No 12*, Vilnius, 2019.

the resilience of critical infrastructure is a top priority for NATO, which complements the collective defence clause stipulated in Article 5.

The disruption of energy supply to the member states could affect the security of allies and partners, while also having a negative impact on military operations. These issues should be primarily the responsibility of national governments, to find common directions on energy security and NATO capability development, to contribute to energy security, while focusing on specific areas. NATO is trying to increase its strategic awareness of energy developments with security implications; to develop its competence in supporting the protection of critical energy infrastructure; and to work for the significant improvement of the armed forces energy efficiency.

The resilience of critical infrastructure is enhanced by NATO through situational awareness, but also by enhancing deterrence and defence in expanding the toolkit for addressing hybrid operations[21]. The statement of the 2018 Brussels Summit announced the establishment of support teams against hybrid threats, which provide targeted assistance to the Allies in preparing and responding to such operations. The Declaration also identified support for Ukraine's efforts to strengthen its resistance against hybrid threats, stepping up action on the NATO-Ukraine platform for combating hybrid warfare[22].

One of NATO's core missions – collective defence and cooperative security – must remain as effective in cybersecurity. NATO's current cyber defence policy places emphasis on protecting its own networks, but efforts to date have to be doubled by setting a set of priorities[23]. Taking advantage of the experience of the other member states, as well as of the industrial partners, the North Atlantic Alliance can enjoy a clearer view on cyber security policies and practices that must counteract contemporary threats and challenges.

CONCLUSIONS OF THE ANALYSIS

It is worth noting that the EU has made substantial progress in building the Energy Union by improving its regulatory framework and investing significant funds in strategic energy infrastructure projects. The challenges of developing European energy security are visible through attempts to combat the influence of monopolistic providers, by implementing the existing regulatory framework and solving the energy interconnection gaps.

[21] Duane Verner, Agnia Grigas, Frederic Petit, *Assessing Energy Dependency in the Age of Hybrid Threats,* The European Centre of Excellence for Countering Hybrid Threats, 2019.

[22] NATO, *Brussels Summit Declaration,* https://www.nato.int/cps/en/natohq/official_texts_156624.htm., retrieved on 28.08.2019.

[23] Ioan Manci, Mihai Ionut Rusu, *Securitatea cibernetică în infrastructurile critice – provocări contemporane*, Editura Academiei Forțelor Terestre , *"Nicolae Bălcescu"*, Sibiu, 2016.

The three actors, the USA, the EU and NATO, need to collaborate to support energy market liberalization and transatlantic interconnectivity projects, as strong energy markets are a shield against contemporary challenges and threats. These energy markets require transparency and competitiveness to mitigate threats to energy security. The importance of economic activities and human development requires the guarantee of the existence of natural energy, and the mobility needs will lead to an increased demand of energy, especially of oil and natural gas.

The aggressive behaviour of some energy vectors, through the use of energy resource by the main political-economic actors, creates an international geopolitical tension. To counter these threats, it is necessary to develop priority community projects on infrastructure, support for consistent implementation of rules, increased education for energy consumers, solutions for energy conflicts and joint collaboration for financing European and global energy infrastructure. All of these are essential for contemporary energy security as well as a great opportunity for closer transatlantic cooperation.

The United States of America and the European Union should take into account, with a note of reciprocity, their energy interests, particularly the controversial issues, namely: Nord Stream 2 and US sanctions on Russia. The states involved in the North Atlantic energy security, being also members of a political-military alliance, require the existence of a consistent practice of using the key principles of cooperation. These involve more openness, transparency, inclusion and reciprocity, fully respecting the decision-making and procedural autonomy of the organizations, without interfering with the specific character of the security and defence policy of any member state.

The interconnectedness of these actors, as well as the dynamics of the geopolitical and economic movements in the transatlantic area, demonstrate that they can engage each other in issues related to infrastructure, alternative sources and routes, advanced energy technologies, climate actions, electricity markets, transport sector and sustainable financing mechanisms. This common approach can strengthen transatlantic energy security and will contribute to a reliable, accessible and competitive energy market, which can be a win-win for both sides of the Atlantic.

Due to the socio-economic factors and the efficiency of production and transport, international energy markets have undergone extraordinary changes in the last decade. An important role in these changes is played by the security of these energy markets, which become more competitive and transparent. However, there is still no single unitary global energy market.

BIBLIOGRAPHY

1. ***, European Commission, *In-depth Study of European Energy Security*, Brussels, 2004.
2. ***, European Commission, *Priority: Energy Union and Climate,* Brussels, 2019.
3. ***, European Commission, *Securing Europe's Gas Supply: New Regulation Comes into Force*, Brussels, 2017.
4. ***, European Parliament*, The Impact of Brexit on the EU Energy System,* Brussels, 2017.
5. ***, Federal Energy Regulatory Commission, *Energy Primer: A Handbook of Energy Market Basics*, 2015.
6. ***, International Energy Agency, *Energy Policies of International Energy Agencies Countries: United States 2019 Review*, 2019.
7. ***, NATO, *Brussels Summit Declaration,* Brussels, 2018.
8. ***, NATO Energy Security Centre of Excellence (NATO ENSEC COE), *Energy Security: Operational Highlights No. 12*, Vilnius, 2019.
9. ***, NATO, *Resilience and Article 3*, 2018.
10. ***, Treaty on the Functioning of the European Union, 2012/C 326/01.
11. ***, US Department of Energy, *US-EU Energy Council*, Brussels, 2018.
12. ***, US Department of the Treasury, *Countering America's Adversaries through Sanctions Act,* Washington, DC, 2017.
13. Sanam S. Haghighi, *Energy Security - The External Legal Relations of the European Union with Major Oil and Gas Supplying Countries*, Oxford and Portland, Oregon, 2007.
14. Ioan Manci, Mihai Ionut Rusu, *Securitatea cibernetică în infrastructurile critice-provocări contemporane*, Editura Academiei Forțelor Terestre *"Nicolae Balcescu"*, Sibiu, 2016.
15. Alexander Mercouris, *Russia Wins Energy War in Europe after EU Surrenders on Nord Stream 2*, 2017.
16. Ellen Scholl, *The Future of Shale: The US Story and Its Implications*, Atlantic Council, 2019.
17. Aaron Sheldrick, *Destination Clauses on LNG Will Soon Fade Away: Gas Union President*, Reuters, 2015.
18. Frederic Simon, *Cañete sees gas as 'a bridge' to reach EU's clean energy goals*, Euractiv, 2019.
19. Duane Verner, Agnia Grigas, Frederic Petit, *Assessing Energy Dependency in the Age of Hybrid Threats,* The European Centre of Excellence for Countering Hybrid Threats, 2019.

A REALISTIC APPROACH TO POWER RELATIONS BETWEEN THE USA AND RUSSIA IN THE CONTEXT OF THE CURRENT WORLD ORDER

Eugen LUNGU, PhD

Lecturer, "Titu Maiorescu" University, Bucharest

After more than three decades of bipolar epoch, followed by the fall of the Berlin Wall, the United States of America became the unique superpower in international relations. Currently, there is a multipolar era, in which the world power has distributed to many actors in the international arena. The United States of America and the Russian Federation are two of the greatest powers of the new multipolar epoch, whose state-of-the-art geostrategic relationships will influence the way the world order in the 21st century will be configured. Russia's opposition to Washington's actions in the post-Cold War era is one of the causes that gradually resulted in the transition to a multipolar era in the international system. The present paper briefly presents, by the political realism perspective, the dynamic of the USA and the Russian Federation power relations, in the context of the current multipolar world order.

Keywords: United States of America, Russian Federation, multipolar world order, military power, political realism.

INTRODUCTION

The end of the Cold War represented, from the perspective of international relations theory, the ending of the bipolar era and the transition to a unipolar system of power with the United States of America as the only superpower of world politics. In this way it was ended an epoch of more than four decades during which, despite the major crises between the West and the East, there was no major military confrontation between the United States of America and the USSR, a historical period that offered a number of theoretical arguments for researchers to consider the bipolar systems as the most stable for world peace. Moreover, the USSR, one of the two pillars of the balance of power during the Cold War, disappeared, its place being taken by the Russian Federation that not only replaced the URSS in the international organisations but also inherited the entire nuclear arsenal owned by the Soviet power.

The dissolution of the Soviet Union, in December 1991, as well as the collapse of the communist bloc in Central and Eastern Europe, reopened the debate in the theoretical space of international relations concerning the polarity system, given the spectacular changes occurred concerning the distribution of world power. The post-Soviet era was characterised primarily by the unilateral dominance of the United States of America in the international system, as well as by Washington's ongoing efforts to promote the principles and values of the liberal order all over the world. The huge power of the USA in political, economic, military, technological as well as other fields has made Washington impose its own vision as a leader of world politics, even though in many situations American interests have collided with those of regional powers, such as the Russian Federation and China.

Although a significant part of the world manifested an opposition to American views in the political, economic and security fields, in the context of the US strategy to implement the values of the liberal order, Washington has often created the impression that it can act as a world government, especially because of its huge ability to project military power anywhere on the planet. The conduct by the US power of humanitarian military operations, as a solution to limit the proportions of humanitarian disasters and to put an end to armed conflicts in some regions of the world, is one of the important features of unipolar world after the Cold War. Washington's armed involvement for solving humanitarian crises as well as the permanent fight against terrorism in the Balkans, North Africa, Central Asia and the Middle East, in the years of the unipolar era, from the perspective of its manifestation as the only superpower in world politics, despite having beneficial

effects on certain categories of populations that suffered because of local wars, or dictatorial regimes, also led to a sense of rejection of the excessive power of the United States of America by emerging powers such as Russia and China. Thus, the wars in Kosovo and Libya, in which NATO forces participated, as well as those in Iraq and Afghanistan, based on US-led coalitions of states, were events that created a sense of insecurity for some states located in the close areas of the military operations, resulting in the aspiration for multipolar world of regional powers. Moreover, the Iraq war from 2003, which was triggered by Washington without having solid reasons, as it was later shown, has been a sensitive topic for US public diplomacy in recent years, as it has attempted to provide reasons for promoting the war that transformed the geopolitics of the Middle East.

The coming to power of President Vladimir Putin, at the end of 2000, marked the beginning of the Russian era revival in the world politics, in which the Kremlin gradually adopted security and foreign policy strategies aimed at weakening the global influence of the United States of America, also favouring the transition to a multi-polar international system.

The courageous strategic objectives assumed by the USA, oriented against international terrorism, on the one hand, or towards changing the regimes of some states that supported global terrorist networks, on the other hand, has required for Washington to allocate huge human, material and financial resources, leading, at the same time, to a hostile attitude in a number of states of the world towards the US foreign and security policy. The enlargement of NATO into Central and Eastern Europe, to those regions that belonged to the Soviet sphere of influence, and the transformation of the North Atlantic Alliance in line with the new trends and developments in the global security environment were perceived by Moscow as a threat to the security of the Russian Federation.

There are many authors in the field of international relations who argue that the era of US unipolarism has already gone, and that we are currently dealing with multipolar world politics. In this space of theoretical approaches is included the article published in the summer of 2019, in *Foreign Affairs*, by the well-known American specialist in political science, Fareed Zakaria, who states: *"Unexpectedly, in the last two years the American hegemony has died. The era of US domination was a short time, an impetuous time, of about three decades marked by two moments, each with their decline. It was born against the collapse of the Berlin Wall in 1989. The end, or rather the beginning of the end, was another fall, that of Iraq in 2003 and the slow collapse since then"*[1].

[1] Fareed Zakaria, *The Self-Destruction of American Power. Washington Squandered the Unipolar Moment*, Foreign Affairs, July/August 2019, see https://www.foreignaffairs.com/articles/2019-06-11/self-destruction-american-power?utm_medium=newsletters&utm_source=fatoday&utm_content=20190611&utm_campaign=FA%20Today%20061119%20Issue%20Release:%20What%20Happened%20to%20the%20American%20Century?&utm_term=FA%20Today%20-%20112017, retrieved on 15 September 2019.

In the spirit of this statement by Fareed Zakaria, but also by other researchers who consider that world politics is currently a multipolar one, we will present some aspects of the power relations between the USA and the Russian Federation, now that the world politics has ceased to be dominated only by the American superpower. Our approach will focus on the brief presentation, within the perimeter of realistic thinking, of the concept of world order, but also on presenting the political and military power relations between the USA and the Russian Federation in the context of the new international multipolar system.

ASPECTS OF THE REALISM THEORY REGARDING THE CONCEPT OF WORLD ORDER

The concept of world order is frequently used by researchers in international relations, from various schools of thought, especially because each type of world order has certain particularities from the perspective of political, social, economic, military events and processes as well as some specific features for interstate business. Thus, there are many definitions attributed to the concept of world order, which we have identified in various specialised works, definitions that theoretically capture elements specific to the different types of world order known to mankind, starting with the order established during 17th century by Peace of Westphalia and continuing with the multipolar order that started at the end of the second decade of the 21st century[2]. In this study we will focus on some of the theoretical approaches of the world order from the perspective of the realistic theory.

Considering one of the remarkable representatives of political realism, Henry Kissinger, an eminent diplomat and author of reference works in the field of world politics, *"the world order can be defined as the conception of a region or a civilisation of what exactly the right ordinances and distribution of power considered applicable to the whole world "*[3]. A theoretical derivative of the world order is represented by the international order which, in Kissinger's opinion, means applying the concept of world order to a sufficiently large part of the earth's surface, which would affect the global balance of power. Therefore, we deduce from Kissinger's definition that, in the realistic view, any system of international order involves a series of laws, rules and limitations jointly agreed by the state actors that are part of that type of order, with the purpose of achieving the balance of power, a fundamental concept of the realistic school. In order to achieve two of the fundamental desires of the realists, namely maintaining the balance of power in the international system and stopping

[2] There are many authors in international relations domain who believe that the unipolar era, of American hegemony, lasted about three decades and practically it can be said that in 2019 this historical period ended.

[3] Henry Kissinger, *Ordinea mondială. Reflecții asupra specificului națiunilor și a cursului istoriei*, Editura Rao, București, 2015, p.15.

the hegemonic tendencies of some actors in the system, the world order thought by realists does not exclude a series of constraints, applied by states or alliances, targeting the state actors attempting to unbalance the system.

The realist school offers other interesting definitions of the world order in which we find the explanation of the relations between states from the perspective of human nature as well as of the power relations between state actors. Thus, John J. Mearsheimer, the most important representative of offensive realism, appreciated almost two decades ago that *"The world order that is established at one point is the by-product of the selfish behaviour of the great powers in the system. In other words, the configuration of the system is the unintended consequence of the competition for power between the great powers, not the result of the concerted actions of the states for the organisation of peace"*[4]. Mearsheimer's definition is especially interesting because in his vision the great powers do not deliberately project a certain type of world order, but that order is a result of their actions to maximise power, a consequence of the competition for accumulating as much power as possible in the world. Therefore, the Westphalian order of the 17th century was not *"something"* previously calculated by the great powers of the respective epoch, of which the combatants dreamed of when they started that devastating war, but it was the result of the conclusion of the Treaty of Westphalia, following the Thirty Years' War, which configured the power relations between the participating state actors in the war and established a series of binding principles for the combatant states.

Approaching the essential aspects of strategic history, in the two centuries that followed the French Revolution, the reputed specialist in international relations Colin S. Gray also focuses on the concept of world order, starting from the essential idea that wars have their origins in interwar periods, meaning in those times when some of the international actors believe that a stable world order had been established. Considering it a rather contested concept, Colin S. Gray thinks that the international order refers to *"a stable pattern of relations between states, which express interests, values and norms considered acceptable by the main states (...) It is necessary to understand the international order in three aspects. First, in a descriptive sense: what is or what was the international order? Secondly, it is a normative concept: how should it be? Third, in a prescriptive way: how can it be improved?"*[5]. The author believes that this definition, by its content elements, reflects the post-Cold War world order to the degree it is appropriate for other world orders known to mankind, such as those established after 1815, or after 1945.

[4] John J. Mearsheamer, *Tragedia politicii de forță. Realismul ofensiv și lupta pentru putere*, Antet XX, Filipeștii de Târg, 2003, p.40.

[5] Colin S. Gray, *Războiul, pacea și relațiile internaționale. O introducere în istoria strategică*, Editura Polirom, Iași, 2010, p.305.

The comparison that Colin S. Gray makes between the unipolar world order, post-Cold War, and the other world orders that the history knows after the French Revolution, it is very interesting, especially concerning the war phenomenon that the author describes it very accurately in his works of reference. Thus, the unipolar world order that followed the fall of the Berlin Wall was not the result of a real war and was not decided as a result of a peace conference, as it can be affirmed concerning other world orders known in the history of world politics.

Considering the world order does not necessarily mean peace, as it can be seen from the study of the history of international relations, Gray states that the international order *"exists and works well enough when the main state and other players are able to pursue and protect their interests, in certain ways and to a degree that all, or most, consider acceptable"*[6]. He also argues that if in a certain type of world order power is no longer balanced, and a state or coalition of states are perceived as entities that create an imbalance in the world order, then the other powers in the international system they are in will unite, sooner or later, to constrain actors who endanger the stability of the system. Thus, regarding the current system of international relations from the point of view of political realism, this last idea supported by Colin S. Gray can be found in the strategic partnership between Russia and China, a growing relationship between two major powers of the world stage that aims at counterbalancing the huge power of the United States of America, challenging the liberal order that Washington has developed, step by step, politically, economically, culturally etc., since the end of the Second World War.

ASPECTS OF POWER RELATIONS BETWEEN THE USA AND RUSSIA AT THE BEGINNING OF THE NEW MULTIPOLAR WORLD ORDER

A quarter of a century ago, at the beginning of the post-Soviet era, Henry Kissinger appreciated that the international system of the 21st century would record a contradictory evolution, being marked, on the one hand, by fragmentation, and, on the other hand, by an accentuated globalisation. But the world order of this century, similar to the European order of the 18th and the 19th centuries, believes Kissinger, will contain at least six major powers: the United States of America, Europe, China, Japan, Russia and probably India[7]. It is the vision of a realist, one of the great personalities of the world diplomacy of the last century, who correctly predicted that the period of American domination in international politics in the post-Cold War era would not be prolonged, and would be replaced by a multipolar system.

[6] *Ibidem,* p. 306.

[7] Henry Kissinger, *Diplomația*, Editura All, București, 2013, p. 21.

In the context of the power relations between Washington and Moscow, although different areas have been involved in the past three decades, the power relations between the political and military sectors of the two states, with influences on the global as well as regional balance of power, have a special relevance for the world politics. Because the power resources of the USA and Russia are particularly important in these two sectors, being a real competition between these two great powers from this point of view, we consider that the power ratios between Washington and Moscow in the political and military space have a very high influence on the international politics in the post-Cold War era. Continuing to present a series of elements concerning the power ratios between the two states, from a political and military perspective, I think it can be deduced how the new world order based on multipolarity can be presented.

Both the USA and Russia have considered in the three post-Cold War decades to get as much power as it was possible from the world power, as well as to make important allies, relevant from geopolitical aspects, and to support each other by virtue of common interests and goals. Although at the beginning of the ’90s we can consider that the Russian-American relations were much more relaxed, compared to the Cold War period, as time went by, starting with the second term of President Vladimir Putin, the geopolitical rivalries between Moscow and Washington has got emphasised, Russian-American disagreements increasingly appearing on the agenda of global politics.

Analysing the military power relations between the USA and Russia from the perspective of the realist school in the new multipolar era, we believe that it is absolutely necessary to consider those issues that concern the global balance of power, taking into account the Kremlin’s visible strategy of the past decade to balance American power, without neglecting the regional formats in which Moscow is actively involved. If, for most of the era of American unipolarity, the global balance of power was latent, due to the existence of a single power[8], major events in the international system of that period, with the United States of America in the position of central player, favoured a dynamic of balance including the Russian Federation as well as other regional powers. Why has Moscow played such an important role from the perspective of balance? Firstly, because Russia, by displaying its redoubtable military force, both at the level of speech of the Kremlin leaders and through its military actions in Georgia, Ukraine and Syria, has transmitted to Washington that it can no longer be considered a second hand power, claiming a leading position in the future multipolar world order. And secondly, because Russia’s foreign and security policy, which is extremely well geopolitically oriented, has managed to attract

[8] Christopher Layne, *Pacea iluziilor. Marea strategie americană din 1940 până în prezent*, Editura Polirom, Iași, 2011, p. 10.

a significant number of states into the orbit of Moscow, countries that have been convinced by the Kremlin about the need not to adhere to the principles and rules of the liberal order promoted by Washington. These states are, first of all, some of those located in the *“close vicinity”* of the Russian Federation, which separated from the former USSR, as well as other states located in Europe, Asia, the Middle East, Africa and South America.

Three decades after the fall of the Berlin Wall, in the new international context characterised by the decline of American influence in the international arena, multipolarity as well as the global balance of power have also favoured the reactivation of regional conflicts. Thus, we can affirm that, in the spirit of realist theory, a number of state actors from different regions of the world have opted, in recent years, for a series of security arrangements with the Russian Federation, promoting in their foreign policy the concept of national interest and strengthening geopolitical advantages. In this way, Moscow has concluded partnerships with various states, using this diplomatic tool that certifies the mutual options of developing cooperation relations in the political, economic, military, cultural and other fields, Moreover, as it can be noticed by viewing the *“map”* of the Kremlin partnerships, they provide the Russian state with special geopolitical advantages.

Why was the global balance of power invigorated in the post-Soviet era? A decade ago, the realist author Robert Jervis appreciated that the dynamics of *“balance”* appears in the context of the use of force, threat of force and fear of force[9]. As it is known, the United States of America has used military force in the international arena several times over the past three decades. It was at the origin of the coalitions that used the military instrument in humanitarian operations, as well as against regimes that have supported international terrorist networks. In the spirit of those asserted by Jervis, without being considered a superpower, Russia has resorted to force actions ever since the unipolar era in order to fulfil its objectives subsumed under the national interest, using offensive military capabilities, which has energised the balance at the level of some regions and has had effects in the global security environment.

The concrete actions of Russia in the era of American unipolarity, characterised by the use of military force, since 2008 – the war against Georgia, the illegal annexation of the Crimean Peninsula, the support of separatism and the civil war in eastern Ukraine, the participation in the civil war in Syria supporting President Bashar al-Assad – have undermined the security architecture of the liberal order Washington has tried to fortify in the post-Cold War period. However, from the perspective of the balance of power, both at the global level and in some regions, the military operations of Moscow have energised the balance of power

[9] Robert Jervis, *Unipolarity: Structural Perspective. World Politics*, vol. 61, No. 1, January 2009, p. 207.

and influenced the security strategies of the main state actors of world politics, in the context of the gradual transition to a multipolar era. If we analyse on the basis of statistical information the relationship between the US military power[10] and the Russian Federation[11], in these first years of multipolar world, even if we observe that the US military power is superior[12], especially in terms of quality, considering it only through the prism of strategic nuclear weapons, of the ability to strike with nuclear vectors launched from the ground, air and water, the nuclear forces of the two states are approximately equal. Therefore, we can affirm that there is a balance of power regarding the strategic nuclear forces of Washington and Moscow, which makes the strategic rivalry between the USA and Russia generate mutual concern and fear at the White House as well as at the Kremlin.

The parity regarding the strategic nuclear weapon between the USA and the Russian Federation made Moscow, a few years after the dissolution of the USSR, launch bold actions, in the foreign policy plane, for the forceful return to the foreground of the world policy, in order for its high-power status to be recognised. Moreover, there have often been situations where, using the logic of political realism, President Boris Yeltsin, and especially Vladimir Putin, in their speeches, convey to the world capitals their determination to use nuclear weapons in the situation in which the Russian Federation will be attacked, or the vital interests of the Russian state will be affected. Therefore, in the spirit of political realism, by virtue of which Russia has no friends or eternal enemies, but only eternal interests[13], the Kremlin began to manifest itself as a great power starting in 2008, after the six-day war against Georgia, transmitting a very clear signal to the international community that the *"transition era"* towards the status of high power ended.

The military power relations between the USA and Russia were also highlighted on the occasion of the renunciation, by both states, at the beginning of 2019, of the Treaty on Intermediate-Range Nuclear Weapons (INF). The conclusion of the INF Treaty between the USA and the former USSR in 1987 was a major moment of the Cold War period, one of the cornerstones of the strategic balance between the two superpowers, which contributed to the increase of the strategic confidence between Washington and Moscow. The renunciation of this treaty by Washington

[10] Hans M. Kristensen, Matt Korda, *United States Nuclear Forces*, 2019, Bulletin of the Atomic Scientists, Volume 75, see https://www.tandfonline.com/doi/full/10.1080/00963402.2019.1606503, retrieved on 7 September 2019.

[11] Hans M. Kristensen, Matt Korda, *Russian Nuclear Forces*, 2019, Bulletin of the Atomic Scientists, Volume 75, see https://www.tandfonline.com/doi/full/10.1080/00963402.2019.1580891, retrieved on 8 September 2019.

[12] For example, at the level of 2018 the military budget of the Russian Federation was $ 63.1 billion, while the US military budget was $ 643.3 billion, see https://www.iiss.org/- /media/files/publications/military-balance-2019/mb2019-defence-budgets-branded.ashx?la=en&hash=C560EFFEC61FA0816B61B8A005215F0510F449EC, retrieved on 8 September 2019.

[13] Lord Palmerston, in the mid-19th century, uttered a famous phrase, often exemplified in the realist school: *"England has no eternal friends nor eternal enemies. Her interests remain eternal"*. We believe that in these coordinates the foreign and security policy of the Russian Federation is being considered today.

and Moscow, in the new strategic conditions at the beginning of the multipolar era, besides the very serious effects in the international security plan, is the expression of the fact that both states today perceive the existence of an international system with several major powers. In this context, experts in international relations express the opinion that all such powers will have to participate in the development of the future INF Treaty. By the time a new INF treaty is negotiated and developed, we must say that the Russian-American power relations on this subject are now generating effects throughout the international system, and the other major powers in the system will have to shape their policies in the field of international security, taking into account the new strategic situation generated by the renunciation of this treaty by the countries that initiated it.

Analysing in the spirit of realism the relations between the political power of Washington and that of Moscow, we consider the behaviour of the two states as permanent members of the UN Security Council as one of the relevant indicators in this field. Appreciating cooperation as a secondary *"element"* of relations between states, the realists *"do not completely neglect the study of the United Nations or the European Union, and they do not deny that sometimes limited forms of cooperation occur, and international institutions are significant only to the extent that they allow the states to pursue their own interests"*[14]. In other words, as it has often been seen in the post-Cold War decision-making process in the UN leadership, both Washington and Moscow have vetoed and blocked a number of the world forum resolutions to protect their national interests. Therefore, the relevance of international institutions to the two states, from the perspective of realistic thinking, means promoting their own interests within an institutional framework, and when this was not possible, as it could be seen in the unipolar era, both powers acted unilaterally, even using the military instrument, from the perspective of political realism, without the support of the the UN.

To give two examples in this regard, during the period of US unipolarism, Moscow used its veto right into the UN Security Council, in 1999 to stop NATO's attack in Yugoslavia, in the context of the Kosovo war, and in 2003 to block the US war against Iraq. In both cases, however, Russia's veto right was inefficient because Moscow's veto in the UN Security Council failed to stop NATO-led military operations in Yugoslavia and the US-led ones in Iraq. However, if we consider these two examples, it can be said that Washington and Moscow have competed with each other, at the political level, as permanent member states of the UN Security Council. To the provided examples other similar ones can be added. During the past decade, it can be said that the two states continue to have serious political divergences when their geopolitical and geostrategic interests are affected.

[14] Jill Steans, Lloyd Pettiford, *Relații internaționale. Perspective și teme*, Editura Antet, Filipeștii de Târg, 2008, p. 81.

CONCLUSIONS

In the new multipolar era that began a few years ago, even though the United States of America will continue for many years to maintain a military advantage over other competitors due to the ability of this state to project force at any point on the planet, more and more studies conducted in the field of international relations state that, in the current world politics, important state actors, competing with Washington, have already appeared, states that will not hesitate to allocate huge resources to develop their military force and to position themselves as best in geopolitical and geostrategic terms. Under these conditions, it is understood that multipolarism will lead to a less stable world order, with a more fragile global balance of power, in which the probability of the outbreak of large-scale wars, with the involvement of the main actors of world politics, will increase. If we take into account the fact that both the First World War and the Second World War occurred in the context of times dominated by multipolarism, giving credence to theorists who consider the multipolar systems as the most confrontational oriented, we do not think that they can be reasons of optimism about how the world of the coming decades will be presented from the perspective of security and stability.

Chinese specialist in international relations Biao Zhang's appreciation that *"President Trump does not have a great love for the liberal order"*[15], but especially the policies of the current US Administration withdrawal from some institutions, agreements, international treaties etc., and a more determined orientation toward domestic politics, show that the current power at the White House tends to attach secondary importance to international institutions, compared to former President Barack Obama. The US withdrawal from the Paris Agreement, the INF Treaty, the Nuclear Agreement with Iran have already left a *"hollow"* in international politics, a space that will certainly be occupied by other great powers in future years, leading to the reconfiguration of the multipolar world order in the following decades.

If the current trend in the US foreign policy is to be maintained, we believe that Washington's involvement in international politics will be further influenced by the realist school, as America is the country that will count first and foremost for American citizens – *"America first"*[16], with lower confidence in international institutions compared to previous times. At the same time, Russia, as it has manifested since 2008, will continue President Putin's line of political realism to manifest power and maintain strategic influence in those geopolitical areas in which

[15] Biao Zhang, *Hans Morgenthau, Realist Theory of International Leadership, and the Future of Global Order*, Chin. Polit. Sci. Rev. (2017) 2: 512-530, see file:///C:/Users/admin/Downloads/Hans_Morgenthau_Realist_Theory_of_International_Le.pdf, retrieved on 9 September 2019.

[16] It refers to the foreign policy adopted by President Donald Trump, starting in 2016, a policy based on unilateralism, protectionism and isolationism.

it is competing with the United States of America, as well as to extend its geopolitical influence in regions where it will not perceive the influence of any great power.

It is expected that, with the beginning of the multipolar era, the competition in the military plan between the USA and the Russian Federation will increase, considering that Moscow has gained a strategic advantage over Washington with the annexation of the Crimea and with the intervention in the civil war from Syria, in the camp of government forces, opposite to the US-backed fighting forces. This competition will be further accentuated after the withdrawal of both states from the INF Treaty, in the first part of this year, to be developed in new coordinates under the conditions in which, in practice, the nuclear arms race was re-launched. Moreover, given the categorical differences between the systems of political organisation of the two states, the differences existing between the political, economic, social, cultural and other values, shared by the two countries, we believe that the Russian Federation will continue, through its actions in the international arena, along with other state actors in opposition to Washington's global policies, to erode the foundations of the current liberal order. This commitment of Moscow against the resistance structures of the current liberal order is one of the challenges that the USA will have to provide appropriate responses in the coming years.

BIBLIOGRAPHY

1. Colin S. Gray, *Războiul, pacea și relațiile internaționale. O inroducere în istoria strategică*, Editura Polirom, Iași, 2010.
2. Robert Jervis, *Unipolarity: A Structural Perspective*, World Politics, vol. 61, no. 1, January 2009.
3. Henry Kissinger, *Ordinea mondială. Reflecții asupra specificului națiunilor și a cursului istoriei*, Editura Rao, București, 2015.
4. Hans M. Kristensen, Matt Korda, *United States Nuclear Forces*, 2019, Bulletin of the Atomic Scientists, Volume 75, see https://www.tandfonline.com/doi/full/10.1080/00963402.2019.1606503.
5. Hans M. Kristensen, Matt Korda, *Russian Nuclear Forces*, 2019, Bulletin of the Atomic Scientists, Volume 75, see https://www.tandfonline.com/doi/full/10.1080/00963402.2019.1580891.
6. Christopher Layne, *Pacea iluziilor. Marea strategie americană din 1940 până în prezent*, Editura Polirom, Iași, 2011.
7. John J. Mearsheamer, *Tragedia politicii de forță. Realismul ofensiv și lupta pentru putere*, Antet XX, Filipeștii de Târg, 2003.
8. Fareed Zakaria, *The Self-Destruction of American Power. Washington Squandered the Unipolar Moment*, Foreign Affairs, July/August 2019, see https://www.foreignaffairs.com/articles/2019-06-11/self-destruction-american-power?utm_medium=newsletters&utm_source=fatoday&utm_content=20190611&utm_campaign=FA%20Today%20061119%20Issue%20Release:%20What%20Happened%20to % 20th% 20American% 20Century? & utm_term = FA% 20Today% 20-% 20,112,017.

ENVIRONMENTAL SECURITY AS PART OF THE NATIONAL AND EUROPEAN SECURITY: THE STRATEGIC DIMENSION OF THE "NATIONAL/EUROPEAN FORESTS AREA"

Mădălina Virginia ANTONESCU, PhD
Scientific Researcher, University of Bucharest

Agenda 2030, as major paper assumed within UN framework by member states, consecrates important parts to sustainable development topics, imposing to the states the increasing of environmental quality, to protect it and to preserve it, as a part of the human security and of the enlarged concept of national and global security, too. More precisely, at the beginning of the 21st century, we can accept a connection between the three types of security, due to the effects produced by aggressions on environment or by the lack of public policies implementation (irrespective of governances) on the local communities security, on states, on regions (regional ecosystems), on entire continents, and to the global level. Within the 21st century it is necessary a new understanding of traditional concepts on security, from the perspective of environment and the challenges to which it is exposed, to a larger extent than in other times. The dimension of protecting the forests (inclusively through methods and pro-active policies to gather waste or through reforestation, protecting biodiversity, protecting ecosystems as such) represents, in our opinion, an active dimension of implementing the 21st century strategies related to human and national security. The present paper presents an approach to forest protection at European and national level, starting from the definition of human security, from the perspective of connecting to the security dimension, the environment as part of national security, briefly considering the forests issue, their quality as a part of national and European security.

Keywords: human security, environmental security, European security, Agenda 2030, national strategy of forests.

INTRODUCTION

Human security, a concept that originates in the post-Cold War period, is defined by the doctrine as the type of individual-related security, in terms of the need to react (by the states that hold the monopoly over the legitimate violence, therefore over ensuring the security of the individuals under their jurisdiction) to the day-to-day threats generated not by the use of guns or armed forces deployed by other states, but from a wide range of sources (economic recession, ethnic rivalries, terrorism, political oppression, shrinking of resources, pandemics etc.)[1]. The doctrine specifically lists the "*shrinking of resources*" (including forests) as one of the causes leading to threats against people (human security which entails *elimination or absence of similar threats, from this point of view, as well*). Therefore, it is necessary that the states or the EU implements strategies and measures regarding the elimination of threats against the human security (the shrinking of resources, specifically listed by the doctrine, includes massive and/or illegal deforestations, the sometimes irreversible destruction of the forest ecosystems, at European level), from the perspective of the concepts of human and environmental security, applicable at national and European level. According to the doctrine, the field of human security includes economic security (absence of poverty), food security (access to food resources), health security (access to healthcare and protection against diseases), *environmental* security (*prevention of environmental degradation*), personal, community and political security[2].

The environmental risk is defined by the doctrine as the coefficient of danger to the environment, to itself and to the humanity, with two interconnected facets[3]: the risk of natural catastrophes, and the technological risks generated by the human activity, which is constantly growing (risk of chemical or nuclear explosions, transportation-related accidents etc.), plus the long-term risk generated by introducing damaging substances or by the excessive use of certain products in natural ecosystems (intensive chemical-based agriculture, industrial pollution with heavy metals, gas emissions during road transportation of freight, nuclear emissions or massive spills of waste products in natural environments)[4].

[1] Marie-Claude Smouts, Dario Battistella, Pascal Vennesson, *Dictionnaire des relations internationales. Approches, concepts, doctrines*, Dalloz, Paris, 2006, pp. 493-494.
[2] *Ibidem*, p. 494.
[3] Cynthia Gorra-Gobin, coord. *Dictionnaire des mondialisations*, Armand Colin, Paris, 2006, p. 331.
[4] *Ibidem*, p. 331.

We consider that the threats to the environment have become *systematic, intense, regional, and even global*, at the beginning of the 21st century, requiring reactions, measures, strategies not only at national or local level, but also *at regional and global level.* We consider that currently the national security can no longer be defined and ensured in the absence of *a dimension covering the human security and the environment security.*

In the future, *the natural resources of states* (natural resources which are part of both private and public property, as well as natural resources such as forests, privately owned by individuals or legal entities) must be regarded as *a coherent structure* – from a legal standpoint, as well – *of natural ecosystems, which are a priority for the "green power" of a state.* We consider that a re-assessment of the European environmental policies is particularly required, when compared to other non-European countries, re-assessment focused on the forests; also, both the EU and its member states must *pay strategic and prioritized importance to the forests* (renewable natural resources). Currently, *the topic of forests is incidentally covered by the EU* (under the topic of *"nature and diversity"*), *as a part connected to the CAP (Common Agricultural Policy)* or *by regional policies.* At this point, forests are not topics of *"strategic importance"* for the EU or the member states; there are no strategies *of national security* and European strategies (under the common defence policy, for example) that include the environmental security dimension and the forest security dimension. Forests are not declared *"strategic areas of significant importance"* for the EU or the EU countries; they are treated by the EU not as *"a natural resource of strategic importance"* in the global competition for the *"green power"* (the third type of power after the hard and soft power), but as biomass, particularly as bio-fuel (we note *an obsolete, mainly economic approach*[5], focusing particularly on the *use and exploitation of forests in the EU*, not on the preservation, protection, reforestation and expansion of forests, *as part of a visionary European effort meant to counter the desertification and to counter the environmental vulnerabilities*).

For the 21st century, we consider that *the environmental vulnerabilities will become some of the most important types of vulnerabilities,* with asymmetrical

[5] For example, we note the perspective of the conclusions drawn by the EU Council in May 2014, according to which forests are of *"crucial importance"* not as a strategic resource that needs to be protected and expanded, but mainly as a consumption resources, as biomass (*"Subsequently, the Council conclusions of 19 May 2014 underscore the importance of the forest-based sector for the EU and the crucial role of forests in making possible the structural transformation of society towards bio-based economies"*). Biodiversity, land use and forestry, http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.5.3.pdf, Fact Sheets on the European Union – 2019, 4, www.europarl.europa.eu/factsheets/en, retrieved on 9 August 2019.

impact on the states, and that they will have to be handled from the *security* perspective, being integrated into *innovative strategies* concerning the national and European security, together with attributing a legal and security meaning to certain concepts such as *"environmental risk", "natural resources", "forests", "forest ecosystems", "forested areas".*

Key-documents adopted by UN states at international level, including *Agenda 21* and subsequently *Agenda 2030*, comprise *important sections that explicitly refer to forests*, with recommendations, measures and objectives concerning the need for these specific ecosystems to be protected. *Agenda 21*[6], a document that focuses on the need for the UN member states to adopt a new perspective of the relationship with the environment and more, in the 21st century, defines *a series of general international objectives*, such as: international cooperation to accelerate the sustainable development of emerging countries and internal policies; countering poverty; changing the consumption patterns; the demographic and sustainability dynamics; promoting the development of sustainable housing; *integrating the environment and the development in the decision-making process*. This pillar dedicated to the social and economic facet of the *"sustainable development"* concept is connected to two other pillars: preserving and managing the development resources, strengthening the role of major groups (such as women, indigenous communities and local populations, children and youth, business communities, non-governmental organizations and local authorities) in implementing the principle of sustainable development. Section II of *Agenda 21* includes *subsections particularly focusing on* the obligations of the states signing *Agenda 21*, in terms of countering deforestation and management of fragile ecosystems.

Agenda 21 defines the principle of countering deforestation, as well as principles and objectives regarding the management of fragile ecosystems, such as countering desertification, water depletion, as well as sustainable mountain development. The document considers that there is an intrinsic connection between deforestation and desertification. Deforestation leads to a change in the quality of the environment, reflected by the lower quality of the breathable air, by the increase in the areas affected by the drought, the damaged agricultural lands, the increased risk of floods, the risk of landslides *directly causing vulnerabilities in local communities, regions, as well as states, as they change the relief* (if these areas are confronted with continue and intense processes of massive deforestation – legal and/or illegal – without eliminating and trying to limit the effects, through massive and intense reforestation).

[6] United Nations Conference on Environment &Development, Rio de Janeiro, Brazil, 3-14 June 1992, *Agenda 21*, https://sustainabledevelopment.un.org/content/documents/Agenda21.pdf, retrieved on 10 August 2019.

Agenda 2030[7], another document regarding the sustainable development, also recommends paying more attention to the environmental security, with direct focus on protecting the forests.

ASCENSION OF THE *"GREEN POWERS"* AND THE NEED TO CONNECT NATIONAL AND EUROPEAN SECURITY STRATEGIES TO THE ENVIRONMENTAL SECURITY (SPECIAL PROTECTION FOR FORESTS)

We consider that, in 2019, the European Commission and the defence ministries of the EU states should initiate *a special strategy regarding the human security connected to the focus of Agenda 2030 (the objective of sustainable development), to the environmental security and the EU strategies on European security*[8] (forest protection) – to the extent to which they have already been outlined. At the beginning of the 21st century, the EU member states *should expand their understanding of the concept of "security" to include the perspective of environmental security and sustainable development.* The example provided by other non-European countries, which adopted quickly proactive, responsible policies, *meant to counter the climatic changes, with the purpose of stopping the relief and climate changes, thus protecting the geopolitical importance* (closely related to the *territory*, in terms of *political, economic and military importance, as a source of hard and soft power*), must be analysed carefully and implemented in the EU countries.

The *geopolitical importance of the EU countries as a coherent structure* is also given by the *responsible and proactive manner in which they handle the environmental challenges,* which tend to *change the traditional relief (source of a specific type of power and a certain geopolitical importance of the respective country)*, in the context of intense and expanding atypical meteorological phenomena or climate changes. In the 21st century, it is important *that the EU countries continue to be a consolidated structure of hard and soft power,* from the viewpoint of *their ecosystems and relief, which they are able to protect against the climate aggressions and other environmental aggressions* (irrespective of their type – natural or caused by large-scale industrial exploitation, by human negligence or by a consumption-based economy that fails to recycle and protect the environment).

[7] See https://www.un.org/sustainabledevelopment/development-agenda/, retrieved on 10 August 2019.

[8] Amending the current EU security strategies by adding the environmental protection topic, at EU level and at global level (connecting to *Agenda 2030*) would be necessary, see https://eeas.europa.eu/topics/eu-global-strategy_en, https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf, retrieved on 10 August 2019.

The European Union has paid and continues to pay particular attention to protecting the environment both at European level (by creating European public policies in this area) and at the level of the member states, by encouraging them to implement environmentally friendly policies[9].

The new element which we want to point out is the fact, in the future, *the "sustainable development" dimension* (in the framework created by *Agenda 2030*) *can be connected directly to the EU policies for environmental sustainability* (noting that significant parts of these policies are dedicated to ensuring the sustainability of the cities from the EU countries, seen as *"green cities"* – a concept of *"sustainable urbanism"*, that turns the EU and particularly the northern countries of the EU into one of the most advanced pillars of the *"green power"*, of its capacity as a political entity, and concept connected to a determined territory, seen as a geopolitical power[10] – ensuring a sustainable development, a decrease in the pollution capacity, as well as a refocus on sustainable technologies, for the European cities of the 21st century), *and the national and European security dimension*[11].

This *interconnection among the three concepts* may seem surprising from the standpoint of *a traditional approach* to security; however, it is fully justified by the EU's need to *develop and adjust its defence and European security policy, depending on the new parameters* (environmental security being one of them) and based on the EU member states' need to find solutions to maintain a high level of common security, *even from the standpoint of the new challenges to the environment.*

In our opinion, *the importance attached to the protection of forest curtains*, as well as to *the European forests as such*, the capacities to *ensure their regeneration*, introducing certain *regulations to prohibit and restrict the uncontrolled or massive, industrial exploitation* of the forests in the EU countries must become *one of the top focuses of the future EU policies*, meant to ensure not only a better quality

[9] See https://europa.eu/european-union/topics/environment_en,https://ec.europa.eu/environment/nature/biodiversity/strategy/target3/index_en.htm, retrieved on 10 August 2019.

[10] Silviu Neguț, *Introducere în geopolitică*, Ed. Meteor Press, București, 2005, pp. 5-10.

[11] The necessity to interconnect at the level of the security strategies, originating in our opinion from the *fundamental principles of environmental law* (the principle according to which environmental protection is a major objective of public interest, the principle of integrating the environmental requirements with the other sectorial policies). Art. 135, paragraph 2, letter d/*Romanian Constitution* stipulates expressly the obligation of the state to exploit the natural resources of the country according to the national interest. See Daniela Marinescu, *Tratat de dreptul mediului*, 4th edition, reviewed and improved, Editura Universul Juridic, București, Bucharest, 2010, pp. 58-61, 63. Monitoring and reducing the risks of climate changes, the principle according to which the polluter pays the price, risk management and prevention of the disasters caused by floods or massive vegetation/forest fires, protecting biodiversity as part of the national heritage should be an impulse to create the inter-ministerial groups and groups for European cooperation (at national and at European level), including *the defence* ministries in the decision-making processes and the management of *environment*, seen as *a strategic resource* of a country, respectively of the EU.

of the environment for the Europeans, *but also the EU geopolitical power,* gained by *adding the dimension of protecting the European forests,* which should be declared *"strategic areas"* in the EU's evolved legislation.

In the future, in the context of climate changes, of various aggressions against the European and global environment, *the EU is called to ensure enhanced security for its citizens, seen as both human security and environmental security.* In our opinion, the EU policies on environment[12] should include a special dimension focused on the protection, expansion, renewal and reforestation of the *forests,* dimension covered *by a mandatory European legislation, directly implemented* by the member states. The current level is still predominantly *on the wrong track, as it prioritizes the consumption economy* (beneficial for the multinational companies), detrimental to the European citizens (especially to the *"green capacity"* seen as a combination between the EU's hard and the soft power to define itself as a *"power"* in the terms specific to the future), and it is marked by *acute illegalities between the east and west of Europe, between north and south*, in terms of *legal status of the forests and the capacity, the concrete will of the states* to implement penalties for the protection of forests.

In our opinion, *the forests must be declared "strategic areas" by mandatory European legislation, implemented urgently at the level of the EU countries, indiscriminately.* They need to be protected, renewed and expanded, and forest curtains must be created in order to limit the desert areas forming and expanding on the territory of the EU countries[13].

In the 21st century, the *national* security can no longer be considered outside or by excluding the environmental protection, especially the protection, expansion and renewal of forests. On the same note, the *European* security will impose

[12] The EU environmental policies should be connected to the EU's common security and defence policy, including its external policy. *See the current level, problematic in terms of human and environmental security, displayed by the EU policies*, https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp/64480/new-strategic-agenda-eu-lead-response-global-challenges_en., https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp/67215/eu-leads-global-fight-against-climate-change_enhttps://ec.europa.eu/clima/news/european-union-continues-lead-global-fight-against-climate-change_en- , retrieved on 10 August 2019. *These documents do not pay special attention and do not prioritize the protection of forests*.

[13] See https://ro.stiri.yahoo.com/%C3%AEn-50-ani-terenurile-m%C4%83noase-din-sudul-rom%C3%A2niei-022109290.html, especially the section. *În 50 de ani, terenurile mănoase din sudul României s-ar putea transforma în deşert. Poluare şi neglijenţă în protecţia mediului (In 50 years, the rich lands in the south of Romania might turn into desert. Pollution and negligence, when it comes to environmental protection).* For example, in Romania, an EU state, the counties Olt, Teleorman, Călărași, Dolj, and Ialomița will turn into sand in five decades, if the areas are not forested, the media warns. Regarding the pollution and renewing the green areas (and countering desertification via reforestation), the EU threatens Romania with huge fines for its failure to observe these obligations. It is necessary to speed up the environmental protection measures, especially in the south of Romania, which is an area threatened by desertification, i.e. a change in relief and climate on this territory, in maximum 50 years.

that the process be reconsidered with the environmental protection as the EU's *"power"* from the viewpoint of *urgently adapting its common security and defence policy to a dimension of environmental security, to the strategic reconnection to Agenda 2030* (and its pillars designed for sustainable development)[14].

In order to become a *"power"* in the evolved sense of the 21st century, the EU as a distinct political entity will have to quickly define a visionary European strategy, meant to guarantee the *"green power"* (the capacity to fight climate change, to reduce the disastrous effects of the aggression against the environment, through responsible and proactive European policies that pay special attention to renewing the European forests).

In one perspective, the territory of the EU countries is the "*EU territory*" *from an economic and sustainable development standpoint, and it must be protected* by a common European security and defence policy, *responsible and extended,* in order to include the *environmental security dimension and particularly the topic of forests.*

In the context of the possibility that the world population increases, of migrations, shrinking world drinking water resources, drop in biodiversity, negative effects of the intensive and chemical agriculture, shrinking forests, which leads to the expansion of deserts, in other words, in the context of the beginning of a food crisis generated by these factors, the EU has the obligation to *rethink its environmental policies, and to connected them to the European security dimension* via *extended* European security strategies *with direct impact on the environment, and particularly on the forest.*

Defining a political entity as a *"green power"* in the 21st century, in this context defined by global aggressions against the environment and lower quality of the environment, by changes in the type of relief caused by the climate changes and the human intervention uncontrolled and tolerated in the name of consumption economy[15], will also depend on *its real capacity to* control and eliminate the threats against the European environment, and particularly against the forests (as *"strategic*

[14] As *Agenda 2030* is considered a key-document, through which the signatory states intend to manage *a global issue* (countering the underdevelopment and countering the waste generated by the consumption economy and generating social inequality at global level). *Agenda 2030 (which also addresses the environmental issue)* becomes a global document, which initiates *a regime of global governance*, due to the fact that the doctrine considers the aggressions against the environment to be global threats. See Jean Jacques Roche, *Relations internationales*, Université Paris II, 3 ed., LGDJ, Paris, 2005, pp. 250-252. The doctrine includes the forest in the category of renewable natural resources. According to Cf. Cynthia Gorra- Gobin, *Dictionnaire des mondialisations*, op. cit., pp. 326-327.

[15] To view the drastic changes in environment and relief caused by human activities and aggressions against the environment: 10 Shocking Photos of Earth THEN and NOW found by NASA, https://www.youtube.com/watch?v=qGaPc7B1mCI, retrieved on 20 August 2019.

areas" that define EU's *"green power"*).

We are looking at the *context of* uncontrolled, global spreading of plastic, insufficiency or complete lack of plastic recycling industries in certain European areas, lack of European legislation – directives, regulations – mandatory for the EU countries, imposing the creation of a plastic recycling industry, the mandatory and large-scale collection of plastic wasted in industrial quantities, in tons of waste products polluting the environment (in rivers, forests, lakes, seas and oceans).

We are looking at *a context in which the consumption economy*, currently insufficiently controlled by ethical and legal environmental protection and quality regulations, *has caused the abuse of* the European ecosystems, *ignoring their strategic and security importance both for the EU and for the EU countries as such, with impact on and reducing the EU's importance as a "green power"* in relation to other power hubs that have an intense and planned focus on the *"green power"* dimension (China, India)[16], via true national policies and sustainable development strategies.

In the competition for the new power (the *"green power"*), which will make a difference in the 21st century *global* competition for power, in the context of the global food and water crisis, of more intense climate changes, massive deforestation, pollution of oceans and general deterioration of the natural ecosystems, the Asian and the African countries, which focus on a harmonization of the political power, of the human society with nature (the concept of *"harmonious society"*), already have a well-defined strategic advantage. Countries such as India, Iran and China are increasingly more focused on adopting public policies, strategies capable of ensuring the development of this *"green power"* meant to give them a geopolitical head start in the 21st century competition[17].

When looking at Asia's strategic advantage, coming from a specific philosophy of *"harmonious cohabitation with nature"*, we consider that the EU has not developed sufficiently and is not sufficiently preoccupied with the environmental policies

[16] Watch the documentaries which approach this issue directly (the rise of the green powers as specific types of powers in the 21st century): *Earth is Greener Largely thanks to China and India, NASA Satellite Study Finds*, https://www.youtube.com/watch?v=iw4cWe8afU8; *China and India Shock NASA by Turning Earth More Green than Before*, https://www.youtube.com/watch?v=6Ixu5WIkfLw, retrieved on 5 September 2019.

[17] Watch the documentaries on the rise of the green powers and the global fight against desertification, to reforest and recreate a friendly environment: https://www.nationalgeographic.com/news/2017/04/china-great-green-wall-gobi-tengger-desertification/, https://www.youtube.com/watch?v=4xls7K_xFBQ, https://www.youtube.com/watch?v=EOSFKGay5Hg, https://www.youtube.com/watch?v=b6ov65o8ZFQ, https://www.youtube.com/watch?v=7Nur35fnjDA, https://www.youtube.com/watch?v=8rQAXaaU1v8, https://www.youtube.com/watch?v=ofxVPChNjTE, https://www.youtube.com/watch?v=-lx92rgo9jo, https://www.youtube.com/watch?v=ACUUIPE2Odw, https://www.youtube.com/watch?v=nak-UUZnvPI, https://www.youtube.com/watch?v=OpUl00vUsAk, https://www.youtube.com/watch?v=IDgDWbQtlKI, retrieved on 6 September 2019.

connected to the common security and defence policy, as well as with the topic of *reforestation and expansion of forests*.

The climax of the consumption economy as a global model *is starting to wear off, displaying the disastrous effects* generated by the massive interventions on the natural ecosystems, as well as *the need to recover and protect them*, as a *strategic approach* adopted voluntarily by the countries and political entities that want to matter 21st century global political environment.

Despite the EU policies adopted, they are *still not regarded as a distinct and essential strategic dimension of the new European common security and defence policy*, as a dimension of the *"green power"*, which should define a Union capable of playing the new global game of the 21st century, a game in which the *"green dimension"* becomes *"power" in itself*, distinct from the hard power and the soft power, but influencing both. *The lack or shrinking of the forests in the EU countries will have a negative impact on the entire European Union, turning it into a global actor incapable of playing the same political game as countries far advanced from this standpoint* (the dimension entailing strategy and security of the forest areas), such as India and China, and will *render it incapable of stopping the changes in relief* (desertification caused by the massive deforestation and the lack of renewal and reforestation), *with negative impact on the EU economy and its power of negotiation* (vast territories, entire mountains turned into deserts, covered in litter, with toxic landfills filled with non-recyclable waste products, prove the need to move past a superficial approach regarding the EU environment and *its geostrategic importance*, *essential* for redefining the EU's role in the 21st century global power game). For the EU and its policy, *abandoning the forests* is not only an infringement of *Agenda 2030*, but also an incapacity to assume a proactive *"green power"* position, with the EU being stuck with the position of *"energy consuming power"*, instead of being the *"green energy generating power"*. As a *"green energy generating power"*, the EU should *focus on* adopting policies regarding: the collection of toxic waste products from forests and mountains on the *"European territory"* (which it risks turning into a third world *"territory"*, from the standpoint of *"green powers"*); reforestation of the mountains and areas that have been massively deforested; penalizing the EU states that have tolerated and encouraged massive deforestation through lax regulations or intricate bureaucratic and procedural mechanisms; building green walls (protection forest curtains meant to protect the cities, water flows, the infrastructure, the rich agricultural areas etc., to expand and ensure the rich areas and to counter desertification).

As an entity with a *"territory"* (particularly in the southern part) mostly arid, turned into a desert as a result of an uncontrolled consumption economy, of industrial, prolonged exploitation, without taking measures to protect and renew

the forests and the environment, the EU can no longer be defined as a *"green power"* in the global power game, when compared to the environment policies and national security strategies advanced from the standpoint of being connected to the environmental protection strategic approach, already adopted by China, India, Russia, and even African states[18]. *The responsibility for the environment, adopting sustainable policies countering the desertification, and the reforestation process become strategic elements of the new policies of national security, meant to ensure the "green power" of the respective country/political entity in the 21st century.* It is surprising that so far, the EU *has not connected* its *environment* policies to the strategic security dimension, to PESC, and has not created a European legislation, European strategies, mechanisms and specific institutions to develop its *"green power" as a geostrategic and security component, as a global projection, as well*[19].

The EU should have used *strategic terms* to define the territories of the member states *that comprise forest ecosystems*[20]*, and should have adopted policies regarding expansion, reforestation, renewal of the forests, collection of the toxic and plastic waste products spread* in their soil and subsoil, in their aquifers and surface waters[21]. If we look at the situation from this viewpoint as well, in terms of

[18] See https://www.unccd.int/actions/great-green-wall-initiative, https://www.greengrowthknowledge.org/resource/building-africa%E2%80%99s-great-green-wall-restoring-degraded-drylands-stronger-and-more-resilient, retrieved on 5 September 2019.

[19] See https://sdg.iisd.org/events/first-great-green-wall-global-conference/, retrieved on 9 September 2019.

[20] See https://ec.europa.eu/environment/nature/biodiversity/strategy/index_en.htm, retrieved on 9 September 2019. The attention paid to forests is *indirect and occasional*, in the topic of *"protecting the biodiversity"*, as the forests as such are treated as *an agriculture-related objective, a subtopic of the objective to preserve biodiversity*. Forests are not included in a particular EU strategy, and they do not benefit from special protection; they are not covered by even one special chapter in the EU strategy on biodiversity or its strategy on the green infrastructure: *"The EU Biodiversity Strategy aims to halt the loss of biodiversity and ecosystem services in the EU and help stop global biodiversity loss by 2020. It reflects the commitments taken by the EU in 2010, within the international Convention on Biological Diversity"*. The term *"forestry"* is currently included in the UE policies as a CAP (Common Agricultural Policy) component, regarded as a pillar (among others) that ensures the EU biodiversity. See https://ec.europa.eu/environment/nature/biodiversity/strategy/target3/index_en.htm, retrieved on 9 September 2019. However, two specific actions that mention forests cannot replace the need for a special strategy dedicated to the EU forests.

[21] Regarding the EU strategy for the forests, it is rather obsolete (dating back to 2013) and it acknowledges that there is no coherent legal framework applicable to all the forest areas in the EU countries. Barely a quarter of the forest areas of the EU is protected through a programme, Natura 2000. In addition, the strategy admits that the process of returning private property (including forests) is ongoing in many EU states, which leads to different legal situations in terms of exploiting the forests. It is also admitted that the deforestation leads to a shrinking of the forested surface in the EU, in parallel with the intensification of forest exploitation rates (by over 30% until 2020). However, the strategy focuses on a sustainable management of the forests, viewing them mainly from *the perspective of their economic use, as bio-fuel, as biomass*, instead of focusing on the protection element and on the expansion of the forestation process, on the actual protection of the forests: *"Nearly a quarter of the EU's forest area is protected under Natura 2000, and much of the rest is home to species protected under EU nature legislation"*, see https://ec.europa.eu/agriculture/forest/strategy/communication_en.pdf, retrieved on 9 September 2019.

a bureaucracy which should have met the needs of the citizens, as well as the EU's need to be able to define itself as a *"green power"*, *such strategic and legislative directions should have been assumed already.* However, *we note a state of inequality and the implementation of legal frameworks displaying significant differences in approach on the topic of forests*, among the different states of the EU, in terms of protection and strategic importance paid to the *forests*. In other words, we are dealing *with national legal frameworks different* in terms of protecting the forests, *not harmonised to be part of a coherent structure, of a "European ecosystem",* bearing this name strategically as a *"strategic area"* meant to be covered by the *European environmental security.*

There is no European security in terms of environment, to pay special importance to the protection of all the forests[22] *and forest ecosystems on the EU territory*[23] by harmonising the legal frameworks and imposing a *unique framework* of clear penalties for the EU states that do not adopt quickly policies and measures for the protection of their forest areas or that do not expand these areas or clear them of toxic and non-degradable waste products[24]. Between the north and the south, between the east and the west, we note a *variety of forestry legal frameworks in the EU*, some of which not being implemented in fact and leaving room for true clandestine industries involved in massive deforestations, organized as true criminal or quasi-criminal networks, tolerated by the state authorities, lax legal frameworks,

[22] See https://ec.europa.eu/environment/nature/natura2000/index_en.htm, retrieved on 9 September 2019. The forests are mentioned in the *"Environment Policies"* section, *"European Commission"* under *"Policies"*, in the *"Greening other areas"* subsection (therefore under miscellaneous). We learn about an EU strategy regarding the forests, but this strategy continues to be included in …. *the common agricultural policy* and as a part of the EU's environment policy, https://ec.europa.eu/environment/forests/index_en.htm, retrieved on 10 September 2019.

[23] See https://ec.europa.eu/info/energy-climate-change-environment_en. If we go to the *"European Commission"* section -> *"Environment policies"* -> *"Topics"*, there is no special subsection focusing on the protection of forests, although other subjects (agriculture, land and soil, transport, wastewater, nature and biodiversity) are expressly mentioned. The *"Nature and biodiversity"* subsection includes links concerning the EU strategy on the Green Infrastructure or the 2020 EU Strategy regarding the Biodiversity; however, forests are not mentioned as such, neither are the corresponding strategies. There are only mentions of concepts such as nature, biodiversity, green capital, green infrastructure, which are addressed from a rather economic perspective, instead of being addressed from the perspective of actual environment protection (green economy, alternate economy), see https://ec.europa.eu/environment/nature/ecosystems/strategy/index_en.htm, https://eur-lex.europa.eu/resource. html?uri=cellar:d41348f2-01d5-4abe-b817-4c73e6f1b2df.0014.04/DOC_1&format=PDF, retrieved on 10 September 2019.

[24] See http://www.mmediu.ro/app/webroot/uploads/files/2017-10-27_Strategia_forestiera_2017.pdf), retrieved on 12 September 2019. The Forest Strategy 2018-2019 issued in 2017 by the Romanian Government acknowledges certain fundamental aspects regarding the current state of the EU policies and strategies regarding the European forest resources: *"Although the EU does not have a joint forestry policy in place, a forestry strategy was adopted in 1998, outlining the importance for the society of the multifunctional role of the forests and of their durable management. At the same time, it stipulates that, although the forestry policy is under the jurisdiction of the member states, the EU can contribute to the GDP implementation through joint policies, based on the principle of subsidiarity and the concept of joint responsibility"*.

as well as public authorities – at local and central level – excessively tolerant of these industries responsible for the massive deforestation and pollution with waste products of the mountains, forests and streams on the territory of the EU countries.

The fundamental concept of *"environment crime", "trans-border environment crime" or "environment organized crime" is neither defined, nor used* at the level of the EU countries or the EU; therefore, the Criminal Code of the EU countries does not stipulate punishments for crimes of this nature or *strategies* at the level of the national defence ministries or the European Commission, at the level of the EU High Representative, *regarding the joint security and defence policy, which also includes the "forestry security" dimension, seen as a dimension of human security, national and European at the same time.*

Besides playing a role of ecological stability and an economic-social one, the Romanian forests, which represent almost 27% of the total surface of the country, must also be regarded more and more from the *extended perspective of the concept of sustainable development, connected to the human security, and the national and European security. For the entire European Union, the forest resources represent a strategic natural resource*[25], which must benefit from a *seamless legal* framework[26] designed to protect, preserve, renew and expand it, and from *a set of clear objectives* to eliminate the legal discrimination among the EU countries and to *align the penalization framework, in case of massive, excessive or illegal deforestation*[27].

[25] According to the EU documents: *"The EU currently contains 5 % of the world's forests and EU forests have continuously expanded for over 60 years, although recently at a lower rate. EU Forests and OWL now cover 155 million ha and 21 million ha, respectively, together more than 42 % of EU land area"*. GREEN PAPER On Forest Protection and Information in the EU: Preparing forests for climate change SEC (2010)163 final, see https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0066&from=EN, retrieved on 12 September 2019.

[26] Starting from a seamless legal definition of the forest and other forested lands. For example, the definition in *GREEN PAPER on Forest Protection and Information in the EU: Preparing forests for climate change SEC (2010)163 final - Forest: "Land with tree crown cover (or equivalent stocking level) of more than 10 percent and area of more than 0.5 ha. The trees should be able to reach a minimum height of 5 m at maturity in situ"*. Other wooded land (OWL): *"Land either with a tree crown cover (or equivalent stocking level) of 5-10 percent of trees able to reach a height of 5 m at maturity in situ; or a crown cover (or equivalent stocking level) of more than 10 percent of trees not able to reach a height of 5 m at maturity in situ and shrub or bush cover"*, see https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0066&from=EN, retrieved on 12 September 2019.

[27] However, the 2018-2027 *Forest Strategy* issued in 2017 by the Romanian Government mentions certain measures and action plans at the EU level concerning the illegal deforestation and illegal wood commerce (there is not, however, a European Forestry Code or a seamless European penalization legal framework in this field, although the institution of the European Prosecutor, a supranational institution which, in our opinion, should be assigned clear competences in this field, as well, will become operational in 2020). *"The action plan for FLEGT represents the policy of the European Union to counter the illegal deforestation and the related commerce. It includes measures concerning the offer and the demand, in terms of the illegal forest exploitation, resulting in two key regulations: a) 2005 – the FLEGT Regulation regarding the control of wood entering the EU from countries that are part of FLEGT (VPA) bilateral voluntary partnership agreements with the EU; b) 2010 – (EU)Regulation no. 995/2020, issued by the European Parliament and Council on 20 October 2010 to set the obligations of the operators that introduce wood and wood-based products on the market, a global measure to ban the distribution on the local market of wood and wood-based products obtained illegally, with the objective to counter illegal wood cutting and related trade"*.

For Romania, the forestry development strategy[28] must be modified and updated to be compatible to the objectives of sustainable development at international level, in the forestry sector, stipulated in *Agenda 2030*, in the *Earth Charter* (adopted in 1992, after the Rio Summit)[29], in the *Convention on Climate Change*[30], in the *Convention on Biological Diversity*[31], in the *Convention to Combat Desertification*[32], in the *Declaration of Principles on the Preservation and Exploitation of Forests*[33] (particularly dedicated to the preservation of tropical forests, which have been painfully exploited lately; the document can also be used as a general framework for other types of forests, as well)[34].

According to the *Convention on Biological Diversity*, *the states have the obligation to take measures to protect the ecosystems,* assuming the responsibility to create *"protected areas"*.

The *Rio Declaration* issued in 1992[35], regarding the sustainable development, which coined the concept of "*quality environment*", stipulates that the states and the peoples must cooperate in good faith and out of solidarity, to implement the principles defined in the Declaration and to develop the international law in the field of sustainable development (principle 27).

Romania must also take into consideration its obligations as a signatory state, regarding the implementation of the strategy for sustainable development of the forests, obligations assumed at the Ministerial Conference on the Protection of Forests in Europe (Helsinki, 1993), as well as the pan-European criteria and indicators for the durable management of forests, adopted at the Ministerial Conference on the Protection of Forests in Europe (Lisbon, 1998) and Vienna (2003)[36].

[28] The 2018-2027 *Forest Strategy* issued in 2017 by the Romanian Government. This strategy does not comprise any chapter on the harmonization or coordination with the objectives concerning the forests, *covered by Agenda 2030, Agenda 21 and any other international documents, signed and assumed by Romania as a UN member and more*, in the field of sustainable development and environmental protection. The strategy focuses only on aligning with the *European and the national* regulation framework. It should be amended with national plans including additional measures, *which permanently focus on aligning with the UN documents in the field and with other obligations assumed by Romania at international level, between 2018 and 2027*.

[29] Daniela Marinescu, *quoted op.*, p. 18.

[30] See https://unfccc.int/resource/docs/convkp/conveng.pdf, retrieved on 12 September 2019.

[31] See https://www.cbd.int/doc/legal/cbd-en.pdf, retrieved on 12 September 2019.

[32] See https://www.unccd.int/, https://www.unccd.int/sites/default/files/relevant-links/2017-01/UNCCD_Convention_ENG_0.pdf, retrieved on 12 September 2019.

[33] See https://www.un.org/french/events/rio92/rio-fp.htm, https://www.un.org/french/events/rio92/aconf15126vol3f.htm, retrieved on 12 September 2019.

[34] Daniela Marinescu, *quoted op.*, p. 20.

[35] See https://www.un.org/french/events/wssd/pages/cnued.html, https://www.un.org/french/events/rio92/rio-fp.htm, retrieved on 12 September 2019.

[36] Daniela Marinescu, *quoted op*., p. 256.

Mădălina Virginia ANTONESCU

INSTITUTIONS AND MECHANISMS FOR THE MANAGEMENT OF AN EXTENDED EUROPEAN STRATEGY REGARDING THE PROTECTION OF FORESTS

From the perspective of combining the concept of *"sustainable development"* with the national and European security, concerning the forest resources of the EU countries, we can say that *a future strategy for the forests of Romania, as a EU member, as well as a future strategy for the forests of the EU*[37]*,* for the 2020-2025 period, should include objectives and measures *much more drastic and concrete, imposed as obligations*, implemented by the member states, in a *seamless legal framework* that stipulates: countering national and trans-border criminal activities involving the environment and particularly the forests; a drastic limited framework concerning the exploitation of the forests in the EU countries; defining the *"European forest resource pool"* as being formed of the forest resources of the EU countries; defining the EU competences in the field of direct *protection* of the *"European forest resource pool"*, as part of the EU cultural, economic, and social heritage; adopting a *European Forestry Code* (which sets up a *general* legal framework for the protection of forests that are part of the *"European forest resource pool"* and unified penalization measures, *at the level of the entire EU*; the national and European *institutions and mechanisms*, and *the cooperation methods for them*, in the field of managing and protecting the *"European forest resource pool"*; setting the European environmental policy as *a priority policy* for the entire EU (from the perspective of the threats posed by the climate changes and the change in quality suffered by the environment and life, in the EU countries, also considering the irrational exploitation and the continuous robbing of the forest resources, associated with the failure to take the proper measures for the protection and renewal of the national forest funds); *connecting* the national forestation programmes to *a European program for the forestation and expansion of the forest funds* (as a concrete measure to stop the massive deforestations and the advancement of desertification, the landslides, the landslips, the massive floods, the atypical or prolonged drought periods, the changes in the natural quality of the forest soils, the air quality, the quality of the environment in the EU countries).

[37] The 2018-2027 Forest Strategy issued in 2017 by the Romanian Government admits that a *"a process of pan-European policy was initiated for the durable management of the European forests"*, which *"is executed in FOREST EUROPE – the Ministerial Conference on the Protection of Forests in Europe (MCPFE). 46 member states participate in this conference, and they elaborate joint strategies meant to protect and ensure a durable management of the forests. Since 1990, 21 resolutions have been adopted and 6 MCPFE have been organized"*, mentions the strategy.

In the 21st century, the *increasingly intense connections* between the climate changes, pollution, massive deforestations, and the national and European human security, as well as the global human security, *require a holistic approach*, in which the EU states must base their actions *both on the objectives set in the international documents on the sustainable development* (for example, the principles of forest protection mentioned in *Agenda 21*), and on the need to create *a seamless European legislation in the field of forest protection, in the entire territory of the EU countries.* The consequences of the drop in environmental quality, the perspectives *of a world air quality crisis* (the forests have a fundamental role in terms of ensuring quality and clean air, not only for the countries where they are located, but also for the entire planet, as a single unique and live ecosystem) *are a direct threat to the human being and the states, from the perspective of security.*

The absence of forests generated by massive deforestation can lead to crisis situations (when entire mountains are deforested), which also leads to the changes in relief, the exposure of the population to natural catastrophes to a greater extent and more directly, to disasters (destructive floods, landslides, landslips, desertification, increased exposure of the agricultural lands to drought, increased air pollution), *all translated as an increase in the vulnerability of the EU states and their peoples* to natural threats (caused by nature, as a consequence of the aggressive, continuous, irrational and massive human intervention in the forests). We could say that, starting with the 21st century, *the climate changes are also the result of direct, industrial-scale human intervention in the forests,* besides the massive industrialization and the warming up of the ozone layer.

The shrinking of forests generates more aggression against the ozone layer, given the low quality of the air and the impossibility to ensure a natural balance in terms of breathable air. *Not only a world food crisis, but also a global crisis of breathable air is foreseeable in the near future,* given the lack of measures regarding de-pollution (including reforestation processes). More and more countries (some categorized as *"third world countries"*, having proved however *that they will conquer their position as "first world" countries, from the perspective of the 21st century principles, focused on the green economy, by implementing visionary strategies regarding the implementation of the sustainable development principles)* implement *consistent national strategies* for the reforestation and expansion of the forest resources, in a national effort to counter the climate changes, *seen as a threat against their national security.*

More and more countries view *the national security from the standpoint of climate changes, which lead to environmental changes, and they start to respond*

to such threats against their security. The environmental security becomes *an intrinsic part of the national security,* for the countries which understand that the climate changes in the 21st century will start to (and already do) generate security issues, with impact on *ensuring the development and prosperity of the peoples, by holding natural resources* ***fundamental for*** the prevention and limitation of negative environmental changes, ***such as in the case of forests***. Countries such as Kenya, Senegal, India, China, France, as well as northern countries in the EU are starting to take concrete measures at national level, ***in order to reforest and expand the forests***, as part of coherent and visionary environmental strategies and of public policies of sustainable development.

The defence of the national and European forest resource pool must become *a fundamental component of the sector of national and European defence.* In the 21st century, the concepts of *"national defence"* and *"European defence"* will also have to include *elements of "defending the environment by protecting the forests"*, especially by expanding and renewing them.

From *the extended perspective* of defence and security, we consider that **an environmental protection department** should be created – considering the various types of aggression (human or natural) against the environment and directly against the forests – **in the defence ministries of the EU countries**; also, **emergency headquarters for immediate response should be created at European level to ensure the protection of forest, and they should be part of the joint European defence headquarters**, in *an accelerated cooperation* among the EU states, *in the field of joint security and defence*[38].

From the extended perspective of the criminal law (including a European competence), the environment and particularly the forests must benefit from a legal framework pertaining mainly to the public law and from a legal framework addressing the private forest properties, *with penalizing and mandatory legal regulations* concerning the conditions of exploitation, the terms and obligations to reforest and renew the forest resource pool and to ensure the improved quality of the forest soil and its waters; *strict and penalizing regulations* regarding the conditions and limitations for the transportation and exploitation of wood; the obligations to ensure the integrity of the forest resource pool and to increase the forested surfaces; implementing the national programmes for the ecological reconstruction of the forests, by the competent authorities, as well as by the entities exploiting the forests; *a strict, penalizing legal framework* for the exploitation

[38] Starting from the current level, in EU, see https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en, https://eeas.europa.eu/sites/eeas/files/pesco_factsheet_may_2019.pdf, retrieved on 16 September 2019.

of forests by companies or individuals and *a highly drastic penalizing framework to prevent* the illegal exploitation of forests (national, local or trans-border networks of illegal forest exploitation), as well as the *legal and criminal responsibility of the authorities for tolerating these types of environmental crime.*

The European programme for the renewal of forests in the territories of the EU states[39], which form the EU forest resource pool, should include *measures applicable to the entire Union, which are mandatory for the EU states,* regarding: forestation of the degraded lands, creation of forest curtains to protect the fields, the communication ways, green areas around the cities, preservation of the forest ecosystems recorded as vulnerable, measures to make wood-exploitation technologies eco-friendly, rational and limited exploitation of the wood, with the obligation to renew the exploited areas and to reforest them, expanding the parks and natural reservations[40] (in the context of intensified climate threats and of the large-scale degradation of the environment and air quality). Similarly, it would also be necessary to introduce *a strict legal framework for the exercise of the property right* (particularly private, but also public) *over the forests*, which is mandatorily *connected to the imperative objectives and measures for environment protection, sustainable development, ensuring the reforestation and, where applicable, ensuring the expansion of the forested areas or building the protection forest curtains.*

Making vulnerable the countries in the EU territory, because of the shrinking of forests or their irrational or illegal exploitation, in the presence of irregular or lax legal frameworks, will lead to *generally making vulnerable the EU as a "green power",* in the context of a competition among the world countries for this type of power, regarding the limitation, shaping, removal of negative effects of the climate changes on the their territory, on their types of relief and their functions. *The environment quality* is influenced by the quality of the forests, by their expansion, by the large-scale reforestation of desert areas, and it has *a direct impact on the national, European and global human security* (given their interconnected nature, in terms of environmental threats).

Since the threats to forests (through illegal or massive, uncontrolled exploitation, tolerated by weak authorities or on account of vague, imprecise legal regulations accompanied by poor penalties) increasingly become national and European threats, requiring an approach which focuses on *the national and European security*, the national security strategies, as well as the European strategy should include *precise*

[39] Currently, there is no such programme in the EU to harmonize the national programmes on the topic of forests, and integrate them in a new approach (although, there is a European forestry strategy, dated 2013)

[40] Daniela Marinescu, *quoted op.*, p. 248.

objectives and definitions of the concepts of *"threats to the environment", "threats to the European forest resource pool"*, as part of the *"strategic natural heritage"* of the EU and the EU countries, the definition of the *"strategic natural heritage"* concept, the definition of the *"green power"* – as a country holding essential natural resources such as the forests, the definition of the *"aggressions against the forests"* – including the asymmetrical aggression among the states, in the competition for the status of continental, regional and global *"green powers"*, the definition of the *"contemporary security environment"* that includes atypical, asymmetrical threats, the definition of the *"threats to the environment"* and of the *"threats to the forests"* – which must also be considered from the standpoint of security, approaching the principle of sustainable development as including the competence to *prevent* the threats to the environment and as a method to *achieve* the national and European security.

An extended European strategy concerning the forests can be a *comprehensive one, entailing* intensified cooperation among the EU countries, in the area of the *joint European defence policy,* as well as cooperation among the states or assigning *the EU direct competences regarding the expansion of the European space of security, freedom and justice*, and cooperation in the area of countering environmental crimes (massive, illegal deforestation activities, including their trans-border aspect). In addition, the protection area can *also be included in the strategies of the EU's foreign policy,* considering that the EU assumes the role of global actor and intends to adopt unified political positions in relation to the non-EU states, at international level, on topics such as the climate change or the global threats to the environment (fires covering large trans-border forests, for example, which require a quick – global – response).

Regarding the *legal relationship between the EU and the EU member states* in terms of developing the area of environmental (forests, in this case) protection, seen as part of *the joint European security and defence strategies, and as part of the European space of security, freedom and justice,* we can suggest creating or defining certain mechanisms and institutions, with certain special competences in the field, such as:

- On the topic of *"trans-border environmental crime"*, the recommendation is to assign a special competence to the European Prosecutor attached to a European Prosecutor's Office[41], based on a *Special European Directorate for all the Environmental Policies and the Trans-border Environmental Crime*;

[41] Based on the current level of competence held by the institution (crimes regarding the EU budget), see https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/networks-and-bodies-supporting-judicial-cooperation/european-public-prosecutors-office_en, retrieved on 16 September.

- European Prosecutors with direct competences in the area of criminal pursuit of the "*trans-border environmental crimes"*, and European Prosecutors with direct competences in the area of criminal pursuit of the *"environmental crimes in the territory of any EU state"*;
- Setting up a *joint subcommittee*, between the institutions of the PESC High Representative and the European Commissioner for the Environment, regarding the accelerated cooperation in the field of a European security strategy with special focus on protecting the forests in the EU countries, regarded as *"strategic areas"*;
- Setting up *joint subcommittee at the level of the Council of Europe* (among the EU states, on the topic of the common strategy regarding forests), with special competences concerning a strategy of the European forest resource pool, as a component of a European strategy of sustainable development;
- *A Special Directorate attached to the European Commission,* to initiate legislation regarding the protection of forests, their de-pollution and expansion, *in direct cooperation with the above-mentioned bodies from other EU institutions, as well as at the level of EU countries*;
- Setting up a *joint subcommittee attached to the European Parliament,* between the environmental commissions and the security commission, regarding the *strategic* environmental security area (with direct focus on the forests in the EU countries).

In addition, there is a series of proposals to be considered, on the following topics:

- The legislative initiative of the European Commission, according to which the environmental policy becomes *a priority* for the EU as such *and is included in the scope of an intensified cooperation among the states*, adding the possibility *to connect it to the joint defence and security policy*, and setting up *combined* institutional and decision-making mechanisms *for the two areas*;
- Setting up a *European Environmental Protection Guard*, which acts in cooperation with a *European Office for the Environment* (institution which receives *enhanced competences* from the EU states, for the activities meant to protect the European environment, *particularly the forests* in the EU countries);
- Setting up *special and intensified* cooperation mechanisms between the European Commissioner for the Environment and the European public servants in charge with implementing the EU joint defence and security policy;

- Setting up a *European Charter of the Environment* (which includes a *European Charter of the Forests*, amended with *a European environmental criminal code*, to define at European level a set of legal principles and regulations concerning the categorization of *European environmental crimes, and the European environmental crime*, with a special chapter dedicated to *the European crimes in the area of forest management and European crime – including trans-border crime – concerning the forests*). Eventually, this legal framework should be included in the *"unique space of security, freedom and justice"* pillar;
- Setting up a *European Prosecutor for the Environment* and a *European court with the jurisdiction to handle litigations in the area of the European environmental law* (including competences to penalize the EU member states when they fail to observe *the European environmental protection legislation, particularly the European legislation stipulating the protection of the European forest resource pool)*.

CONCLUSIONS

As demonstrated above, despite certain steps taken by the EU in the field of forest protection, *currently it does not pay any special attention to or prioritise* its forests, and there is no *consolidated and extended* European strategy to introduce the pillar of environmental security in the scope of European security and of the joint security, defence and external policies, at European level. The forests should be a *"European forest resource pool"*, which receives unified legal protection (via a European Forestry Code and penalization regulations implemented in a uniform manner, at the level of the EU countries). Irrespective of the scenario chosen – considering the environmental security pillar (forest protection) to be part of the *"unique European security, freedom and justice space"* (the European Prosecutor receiving special competencies in the field, especially in the field of countering environmental trans-border crime), or considering it part of an intensified cooperation among the EU countries, in the field of joint security and defence policies – it is essential that the EU quickly defines its vulnerabilities and strategic advantages regarding the environment, particularly regarding the protection of its forest resources and treating them as a *"strategic area"*, protected by a well-defined, seamless legal framework.

BIBLIOGRAPHY

1. ***, *China and India Shock NASA by Turning Earth More Green than Before*, https://www.youtube.com/watch?v=6Ixu5WIkfLw.
2. ***, *Earth is Greener Largely Thanks to China and India*, NASA Satellite study found, https://www.youtube.com/watch?v=iw4cWe8afU8.
3. ***, *GREEN PAPER on Forest Protection and Information in the EU: Preparing Forests for Climate Change SEC (2010)163* final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0066&from=EN.
4. ***, Government of Romania, *Strategia forestieră naţională, 2018-2027*, issued in 2017, http://www.mmediu.ro/app/webroot/uploads/files/2017-10-27_Strategia_forestiera_2017.pdf.
5. ***, United Nations Conference on Environement&Development, Rio de Janeiro, Brasilia, 3-14 June 1992, *Agenda 21*, https://sustainabledevelopment.un.org/content/documents/Agenda21.pdf.
6. ***, World Resources Report, Final Report, July 2019, *Creating a Sustainable Food Future. A Menu of Solutions for Feed nearly 10 Billion People by 2050*, https://www.wri.org/publication/creating-sustainable-food-future-final-report.
7. Cynthia Gorra-Gobin, *Dictionnaire des mondialisations*, Armand Colin, Paris, 2006.
8. Martin Griffiths (ed.), *Encyclopaedia of International Relations and Global Politics*, Routledge, London and New York, 2005.
9. Daniela Marinescu, *Tratat de dreptul mediului*, 4th edition, Editura Universul Juridic, Bucureşti, 2010.
10. Silviu Neguţ, *Introducere în geopolitică*, Editura Meteor Press, Bucureşti, 2005.
11. Jean Jacques Roche, *Relations internationales*, Université Paris II, 3rd edition, LGDJ, Paris, 2005.
12. Marie-Claude Smouts, Dario Battistella, Pascal Vennesson, *Dictionnaire des relations internationales. Approaches, Concepts, Doctrines*, Dalloz, Paris, 2006.

WEBOGRAPHY

1. https://ro.stiri.yahoo.com/%C3%AEn-50-ani-terenurile-m%C4%83noase-din-sudul-rom%C3%A2niei-022109290.html, articolul: *"În 50 de ani, terenurile mănoase din sudul României s-ar putea transforma în deşert. Poluare şi neglijenţă în protecţia mediului".*
2. https://www.tfa2020.org/wp-content/uploads/2017/12/TFA2020_CommoditiesandForestsAgenda2020_Sept2017.pdf.
3. https://www.weforum.org/projects/global-water-initiative.
4. https://www.un.org/sustainabledevelopment/development-agenda/.
5. https://eeas.europa.eu/topics/eu-global-strategy_en.
6. https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf.
7. https://ec.europa.eu/environment/nature/biodiversity/strategy/target3/index_en.htm.

8. https://ec.europa.eu/environment/nature/biodiversity/strategy/index_en.htm.
9. https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp/64480/new-strategic-agenda-eu-lead-response-global-challenges_en.
10. https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp/67215/eu-leads-global-fight-against-climate-change_en.
11. https://ec.europa.eu/clima/news/european-union-continues-lead-global-fight-against-climate-change_en- .
12. 10 Shocking Photos of Earth THEN and NOW founded by NASA, https://www.youtube.com/watch?v=qGaPc7B1mC.
13. https://www.nationalgeographic.com/news/2017/04/china-great-green-wall-gobi-tengger-desertification/.
14. https://www.youtube.com/watch?v=4xls7K_xFBQ.
15. https://www.youtube.com/watch?v=EOSFKGay5Hg.
16. https://www.youtube.com/watch?v=b6ov65o8ZFQ.
17. https://www.youtube.com/watch?v=7Nur35fnjDA.
18. https://www.youtube.com/watch?v=8rQAXaaU1v8.
19. https://www.youtube.com/watch?v=ofxVPChNjTE.
20. https://www.youtube.com/watch?v=-lx92rgo9jo.
21. https://www.youtube.com/watch?v=ACUUIPE2Odw.
22. https://www.youtube.com/watch?v=nak-UUZnvPI.
23. https://www.youtube.com/watch?v=OpUl00vUsAk.
24. https://www.youtube.com/watch?v=IDgDWbQtlKI.
25. https://ec.europa.eu/agriculture/forest/strategy/communication_en.pdf.
26. https://ec.europa.eu/environment/nature/natura2000/index_en.htm.
27. https://ec.europa.eu/environment/forests/index_en.htm.
28. https://ec.europa.eu/info/energy-climate-change-environment_en.
29. https://ec.europa.eu/environment/nature/ecosystems/strategy/index_en.htm.
30. https://eur-lex.europa.eu/resource.html?uri=cellar:d41348f2-01d5-4abe-b817-4c73e6f1b2df.0014.04/DOC_1&format=PDF.
31. https://unfccc.int/resource/docs/convkp/conveng.pdf
32. https://www.cbd.int/doc/legal/cbd-en.pdf.
33. https://www.unccd.int/.
34. https://www.unccd.int/sites/default/files/relevant-links/2017-01/UNCCD_Convention_ENG_0.pdf.
35. https://www.un.org/french/events/rio92/rio-fp.htm.
36. https://www.un.org/french/events/rio92/aconf15126vol3f.htm.
37. https://www.un.org/french/events/wssd/pages/cnued.html, https://www.un.org/french/events/rio92/rio-fp.htm.
38. https://eeas.europa.eu/topics/eu-global-strategy/64480/new-strategic-agenda-eu-lead-response-global-challenges_en.
39. https://europa.eu/european-union/topics/environment_en.

40. Biodiversity, land use and forestry, http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.5.3.pdf.
41. Fact Sheets on the European Union - 2019 4 www.europarl.europa.eu/factsheets/en.
42. https://www.unccd.int/actions/great-green-wall-initiative.
43. https://www.greengrowthknowledge.org/resource/building-africa%E2%80%99s-great-green-wall-restoring-degraded-drylands-stronger-and-more-resilient.
44. https://sdg.iisd.org/events/first-great-green-wall-global-conference/.
45. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en.
46. https://eeas.europa.eu/sites/eeas/files/pesco_factsheet_may_2019.pd.
47. https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/networks-and-bodies-supporting-judicial-cooperation/european-public-prosecutors-office_en.

FOOD SECURITY IN THE CONTEXT OF A GLOBAL FOOD CRISIS AND THE RISE OF "FOOD POWERS" – SEVERAL CONSIDERATIONS –

Mădălina Virginia ANTONESCU, PhD
Scientific Researcher, University of Bucharest

In this paper we will try to analyse the concept of "food security" as part of national security, considering both Agenda 21, Agenda 2030 and the perspectives – already outlined in a recent UN report – on the global food crisis connected with the negative effects on environment, especially regarding the reduction of fertile surfaces and drinking water, due to the extension of desertification, massive forest fires, chemical intensive agriculture, various aggressions, industrial exploitation or large-scale pollution with toxic or non-renewable waste of the environment. In the 21st century, it is possible to develop new concepts related to "power", namely "green powers", which are able to manage their relationship with the environment in order to increase their political decision-making power and geopolitical importance in world decisions (including as "food powers") as well as to provide increased protection and security to their people. These "new powers" are those countries which, from now on, focus on the development of national, even regional agricultural industries, and on the protection of their fertile areas as well as of their ownership over them, areas defined as "strategic areas", in order to ensure, from the surplus of food raw materials, a regional or even global influence, in terms of sustainable development (post-realism).

Keywords: food security, human security, global food crisis, climate change, Agenda 2030.

INTRODUCTION – FOOD SECURITY, AN INTRINSIC PART OF HUMAN SECURITY. THE ASCENSION OF "FOOD POWER"; "FOOD POWER" AS THE NEW TYPE OF POWER RELEVANT IN THE 21ST CENTURY

In our opinion, *food security is one of the pillars of the concept of human security in the extended sense*, as it is connected to another fundamental concept for the 21st century world, *sustainable development*. At the same time, food security is a basic component of *national and European* security (implemented at the EU level through enhanced cooperation between the EU states in the field of CSDP). Food security entails direct, *consolidated and extended competencies for the armed forces in ensuring the effective protection of fertile lands* (in terms of both classic risks, such as inter-state warfare, and non-conventional risks – sudden and massive displacement of populations due to war, hunger, economic issues such as economic migration –, migrants interested in settling and taking possession of the fertile lands, by using them in the territory of the states where they reside as refugees, economic migrants, asylum seekers etc., *regardless of the respective state's approval*). International migration for economic reasons must be controlled and limited by states as well as globally, *in order not to create risks of violent confrontations between local populations and those displaced from their place of origin, who are in search of satisfying food needs* (in the context of the outbreak of wars, food crises and regional or global economic crises due to the demographic explosion or the financial crises that can affect a country or a group of countries).

A special legislation should be considered, as a priority objective for any national security strategy of the EU countries facing the regional, continental or global food crises, with the identification of "food risk areas" for the EU (Balkans, Central Asia, Transcaucasia, Africa, the Middle East) as areas where it is possible for economic migrants to move in massive and constant waves, outside the control of EU states or creating constant pressure on host EU countries, including from the point of view of ensuring access to food and increasing the pressure of cities on the possibilities of rural areas to meet the food needs of European cities affected by this sudden demographic impact.

Likewise, in *the special legislation dedicated to the strategic protection of the property of the EU states on the fertile lands* (to be declared*, in each EU country, "strategic areas", in the context of global and regional food crises*), in order to ensure the status of EU food power, as well as of regional and global autonomous actor, and in the case of such complicated regional and international contexts, provisions should be made for *the prohibition of the acquisition or occupation by foreign populations (as a result of economic migrations) of the fertile lands and forests in the countries of settlement of these populations.* Also, to meet the needs of food and stability (avoiding conflicts with local populations for food needs), *host countries should provide legislation for the activation of special European food solidarity funds (including* ***the creation of a European Commissioner position for the prevention and management of food crises throughout the EU territory****)* but also *national environmental protection legislation* (forests, pastures, agricultural lands) considered as *"strategic areas"* and *"territory of strategic importance"*, also involving the competencies of the armed forces (as a competent force including for the management of unconventional, asymmetrical wars). Ownership of agricultural land, fertile land, regarding the foreigners' access to these lands *should be restricted or limited* from this point of view, given that *food security is part of national security*, imposing a *long-term strategic thinking to ensure security, independence, economic stability of the EU state and of the whole EU, as such* (the economic power of EU states, by ensuring ownership of agricultural land by nationals, should guarantee regional stability, and state control over fertile land, in national interest and European interest).

Food security is also related to the notion of *"environmental threat"* or *"environmental risk"*. Exposed to large-scale industrial activities, sometimes with negative and lasting or even irreversible effects, produced at a cross-border level, the environment is, in the 21st century (also known as *"Anthropocene"*), *exposed to a much greater and more intense extent* than in the past*, to aggressions* caused by the intense and extensive application of *the consumer and industrial society model.* The 21st century will be defined, in our acceptance, more and more by *the need for a reaction at national, regional and global level,* which the states, people and integrated regional assemblies of the EU type will have to adopt in order to *combat, eliminate, and reduce the "food risk".*

We define *"food risk"* as a specific type of risk to nations, people, related to and dependent on *"environmental risk"*. In other words, if the *"environmental risk"* determines the need of nations, states, regional assemblies to *rethink*

the notion of "security", from the perspective of its human, national, regional and global dimension and linking it to the environmental protection dimension, *"food risk"* becomes a concept closely related to food security, thus determining the need to think strategically with regard to national security, human security and environmental security, all being interconnected.

"Food risk" defines, in our opinion, the hazard coefficient generated on a nation of a state, of a local community, of a regional political or economic assembly (of the EU type), due to the various actions (political decision-makers but also companies), industrial, economic and financial crises, wars as well as the *"environmental risk"* (by drinking water depletion, forest depletion, expanding dry and desert areas, climate and relief changes, massive deforestation not accompanied by regeneration measures and the restoration of the destroyed ecosystems, the long-term practice of chemical agriculture, the extension of the urbanisation, the waste disposal in the drinking water and in the oceans and seas, the heavy metal pollution of the terrestrial and aquatic ecosystems, the pollution of the air etc.). From all these *environmental risks* (caused by human action, industrial activities, intensive chemical agriculture as well as by natural disasters or chemical explosions, nuclear results of human activity), result *food risks* (contamination of air, plants, pastures, waters with heavy metal, radioactive or chemical products, toxic or harmful to animals, birds, plants, and humans; pollution with non-recyclable waste of the environment; expansion of drought-affected areas and the depletion of agricultural land and fertile land as a result of deforestation and the advancement of desert or urban areas; depletion of drinking water resources, draining rivers, lakes, contaminating groundwater or drying it due to negative human interference on soil and subsoil; use of toxic substances, pesticides, in plant, vegetable, cereal cultivation intended for animal and human consumption; plastic pollution that becomes a blanket of plastic micro-particles covering the bottom of the seas, lakes and oceans thus suffocating the elements of aquatic ecosystems, entering in the consumption of fish, animals and then of man).

In the 21st century, on the background of the emergence and extension of the clues illustrating *a global food crisis*, a *new type of power* appears and consolidates, modelling the policy of the 21st century according to *"food power"*. Along with soft and hard power, *"food power"* is a distinct type of power, measurable in a state's ability to meet the food security needs of its people but also to ensure strategic food surpluses (cereals, fruits, vegetables intended for human basic consumption) to ensure dominance in food and cereal markets, compared to countries that do not

have this surplus or are discouraged (through internal weakness, strategic economic and food vulnerability, we would say) to own or to use this type of power[1] in a *"political projection"* mode; use of this food capacity to provide surplus and staple food needs *for other countries* (lacking in strategic food resources) to *extend and strengthen their economic and political domination over other countries* (until they form *real spheres of influence, based on the control over the strategic markets of staple foodstuff*, where that state holds a monopoly or dominant position).

In the context of appearing clues of a global food crisis (including due to the growth of the human population by 2050, as estimated by UN reports, at 10 billion[2]), we believe that *the rise of "food power" will be one of the most important features of the global world of the 21st century, as well as the competition between them, for the redefinition of the international system* according to the control over the food markets and the supply of basic products for the 10 billion people, from now until 2050.The report issued in July 2019 by the World Resources Institute shows the need to change the global model of food production and consumption. The concept of *"global agricultural system"* is introduced, which must be connected, in the authors' view, to the concept of *"sustainable development"* and *"human security"*. The need for food insurance for 10 billion people by 2050 is estimated by farmers.

The International Cooperation Principle, the Food Solidarity Principle and National Security; Global Food Risk and Economic Migration – Some Aspects of the Relationship with the Agricultural Sector

The field of agricultural production will become, in the near future, one of strategic importance, directly connected with the field of national security, to ensure basic consumption for the local population.

[1] For example, a Stratfor analysis of Turkey's economic development by 2020 sees it as *a rising economic power, as an agricultural power, capable of projecting power in Southeastern Europe, in the Balkans, to dominate with its agricultural products, vegetable, fruit, captive markets of states that have not exploited their strategic food policy advantages as part of national security* (Romania, Bulgaria, Albania, Greece, Montenegro, Bosnia, Kosovo – countries where the decline of the EU will be increasingly evident in the coming decades, as compared to Turkey's commercial and agricultural expansion in these markets, especially given that, since 1990, with the opening of Eastern Europe, Turkey has been one of the countries that have entered strongly on these Balkan markets with the agricultural products of its farmers). Turkey will be one of the expanding food powers starting in 2020, in direct competition with the EU, Russia and other states in the former Soviet area. See Stratfor.com, 2 July 2012, *Developing Relations between Turkey and Europe*, quoted in Sorin Aparaschiva, *Turkey-Changes and Trends among the Political-Military Elites*, in the anthology of scientific communications *Turkey – from Kemal Ataturk to the EU*, coordinator Guven Gungor, Vasile Simileanu, International Scientific Paper Session, Geopolitica Club Cafe, Revista Geopolitica, București, 8-9 February 2013, Top Form, București, 2013, pp. 22-30.

[2] World Resources Report, *Creating Sustainable Food Future. A Menu of Solutions to Feed Nearly 10 Billion People by 2050*, Final Report, July 2019, see https://www.wri.org/publication/creating-sustainable-food-future-final-report, retrieved on 15 August 2019.

Specific international obligations will have to be assumed by states (possibly, by signing in the future, of some ***International Solidarity Conventions on cost-sharing regarding the consumption and production of staple foodstuff***, starting from the principle of cooperation between people and states for food security for the 10 billion people by 2050), as UN members, as parts of FAO and other bodies, which will need to be set up for management in accordance with the principle of sustainable development, based on an *"after-waste"* (the green economy), including the organisation of a *global industry ensuring the 10 billion people with base products, by 2050.*

The emergence of a global food crisis may be due to the demographic explosion and underdevelopment, the widening of the economic discrepancies between countries, the diminution of agricultural land and water resources. FAO has warned since 2002 that the global consumption society is spending the planet's natural resources to a much faster extent than its ability to regenerate[3]. The poor states will have to adopt (with international financial support) technologies for transition to the green economy and to implement projects of environmental regeneration, extension of forested areas and return to *"green agriculture"*.

The global food crisis leads to *direct risks for national security of states, for global security and for environmental security*. It can cause massive, uncontrolled migrations to countries rich in strategic resources (fertile soils, fertile agricultural lands) and which do not have strong armies or adequate legislation to defend themselves against these asymmetrical threats and economic migrations[4]. According to the doctrine, in the future, the demographic explosion in combination with the migrations will lead to disasters or conflicts unknown in the past as magnitude and will be the basis for the creation of a new international system[5]. The demographic increase to 10 billion in 2050 determines food risk including for the countries rich in strategic resources (agricultural lands, fertile pastures, fertile lands), which become *targets of the great human displacement, which will reconfigure the entire international system as we know it today, giving birth to a new world order.*

[3] Vasile Simileanu, *Geopolitica* și *centre de putere*, Ed. Top Form, București, 2010, p. 81.

[4] Migrations are defined in doctrine as those movements of populations or persons, temporarily or permanently, of their place of residence, both within the internal and international framework (outside the area of jurisdiction of their home states). The doctrine introduces, within the framework of international migrations, economic migrations, generated by the lack of labour or generated by the lack of staple foods that the state of origin had to provide its population. International migrations are based on very large economic gaps between countries, with migration flows being oriented from poor to economically developed countries. Vasile Simileanu, quoted op., p. 95.

[5] Viorel Roman, *Religiile, sursă de conflict*, Ed. Academiei de Înalte Studii Militare, București, 1992, pp. 82-83, cited in Vasile Simileanu, *quoted op*., p. 96.

Economic migrations will replace, as the main risk model, migrations due to political causes, political persecution or wars. *Migrations due to lack of staple foods* will replace migrations based on other reasons. If we look closely at the causes of migration that hit the EU in 2015-2016, we will find that at the initial (Syrian) migration, for reasons of war and political persecution, was added a constant *migratory mass for economic reasons* (lack of functional national food industries, fertile land, staple food insurance, in the original form but also processed in the country of origin, the chronic under-financing of the agricultural sector in the countries of origin), coming from Africa or the Balkans (depopulation of the Balkans, rural areas, economic migrations to cities and to Western Europe, due to the lack of agri-food industries, the functioning chain of production-consumption-recycling of food, necessary for the development of rural and urban areas in the Balkans, and the implementation of the green economy). Similarly, the case of Venezuela and the crisis of 2018-2019, reflects pauperization at a national level, connected with the need to provide staple food for the local population, in the absence of which there has been a massive migration to other countries in Latin America and to the USA. But the case of Venezuela is not unique: other countries facing economic difficulties (including a reduced capacity to ensure the production and consumption of staple food for local populations), from Latin America (Honduras, Guatemala, Haiti, Nicaragua etc.), have determined largely economic migrations (lack of basic needs, among which food, despite the profile of their *"agricultural countries"*), pushing large masses of people to economically prosperous countries (the USA, for example).

Human security will begin to be thought of in strategic terms related to food security, the lack of assurance of this type of security by the states causing *the occurrence of food risks, asymmetrical risks, uncontrolled migrations* to and from a state/region, including the risk of transcontinental migration, from the southern continents, without developed agri-food industries and without natural resources or with highly depreciated natural resources as a result of pollution, uncontrolled deforestation, intensive chemical farming, heavy metal polluting industries etc. (agricultural land, fertile land, for plants intended for human and animal consumption). Even if it is estimated that at present, the world agricultural sector involves 2 billion people who work practically in this field, this is insufficient for the development prospects of this sector but also for its connection with the strategic and security side.

Agriculture, cultivation of plants and fruit trees, providing pastures for herds of cattle, will become strategic sectors of the highest importance in the 21st century, requiring both *environmental* protection (environmental security) but also *legislative and military* protection (the powers of national armed forces, extended for the defence and concrete protection of fertile land and strategic agricultural and forest resources against any threats and attacks, symmetrical and asymmetrical generated by the regional, local or global food crisis, including wars).

It is quite possible that, given this context, UN member states will sign *international strategic conventions* in the future, by which they are *obliged to donate to global food insurance funds, percentages in money and food* for staple food insurance of poor countries, for the prevention of economic migrations, for the restoration of the harmed ecosystems of these countries, for the reduction of desertification and for reforestation.

We appreciate that, in the 21st century, some of the most important aspects of a reformed UN will be *institutions with competencies in the field of managing the needs of agriculture-related states, providing staple food for their populations*, so as to increase solidarity between states and avoid migration, asymmetrical risks and wars generated by local, regional or global food crises. Consumption of strategic resources and increase in the global population, combined with the perpetuation of the consumer economy model, with the lack of measures to prevent food waste and to combat pollution generated by food waste, with the lack of food recycling industries, with the consumption of natural resources (agricultural land, fertile lands, forests) lead to an increased risk of wars, starvation and pandemics generated on this background.

It is essential that states should assume *the principle of cooperation between all states and people in the field* of food waste prevention, combating pollution of agricultural land, fertile areas, expanding fertile areas by combating desertification and by the emergence of industries related to the conversion of saltwater into drinking water.

Some of the most important international conventions of the 21st century, in our opinion, will be those concluded by states on: the prevention of the global food waste; the extension and protection of the fertile areas of the Earth, including by combating desertification; the solidarity between states through their obligations to give up percentages of their GDP to a global food solidarity fund, which will provide people and states without natural resources or with depreciated or drained resources, or in the process of restoration, with staple food; the conventions

for the prevention of economic migration; the conventions for global support of the global agricultural sector through investments in the agri-food industries in developing countries; the conventions for the regeneration of fertile lands, for their protection and extension *as a strategic resource not only of the holding states but also of the whole humanity* (the lack, the diminishing of the fertile areas leading to the extinction of the human species, the biodiversity, to the disappearance of a whole type of society (based on agriculture and livestock farming); an agreement to limit the impact of intensive or chemical agriculture on fertile soils and on the quality of soil and subsoil, to prevent soil degradation, water contamination and to combat the effects of heavy metal industrial pollution and their discharge in areas that have contact with fertile soils.

A globally equitable distribution of foodstuff should reduce global food risk as well as environmental risks, through the *controlled exploitation* of fertile land and through avoiding mass economic migration, the *"urban burden"* that would lead to true asymmetrical threats to the states, for which the traditional concepts related to *"national security"* are not prepared. Specialist estimates concern an increase of almost 50%, by the middle of the century, of the need for food in general, and with almost 70% of the need for meat foods. According to the July 2019 report issued by the World Resources Institute[6], there are three specific challenges of the global food system: food supply (need to increase food production with 50% by 2050); land use (which is related to the need to expand agricultural land, which would mean affecting terrestrial ecosystems, intensifying climate change and threats to biodiversity); gas emissions from the agricultural sector (which can be reduced including by reforestation of at least 585 million hectares of agricultural land)[7].

RELEVANT INTERNATIONAL DOCUMENTS ON FOOD SECURITY

In a key document adopted at the Rio de Janeiro/1992 summit on sustainable development, *called Agenda 21*[8], there are within the first pillar (social and economic dimension) implicit references to *ways of combating a global food crisis, through objectives such as*: international cooperation to accelerate sustainable development

[6] World Resources Report, *Creating Sustainable Food Future. A Menu of Solutions to Feed Nearly 10 Billion People by 2050*, Final Report, July 2019, see https://www.wri.org/publication/creating-sustainable-food-future-final-report, retrieved on 10 September 2019.

[7] *Ibidem.*

[8] *Agenda 21, United Nations Conference on Environment &Development, Brazil, 3-14 June 1992, United Nations, Sustainable Development*, see https://sustainabledevelopment.un.org/content/documents/Agenda21.pdf, retrieved on 10 September 2019.

in developing countries, accompanied by appropriate internal policies; fighting poverty; changing consumption patterns; demographic dynamics and its connection with sustainability; promoting and protecting human health conditions; promoting the sustainable development of human settlements; integrating the environment and development into the decision-making process. Also, in the second pillar of the concept of *"sustainable development"* are met *objectives related directly to combating a global food crisis*: an integrated approach on the planning and management of land resources; combating desertification and drought by managing fragile ecosystems; promoting sustainable agriculture and rural development; protection of quality and the supply of fresh water resources; management and use of water resources; preventing the illegal international traffic of toxic and dangerous products, within the management of toxic chemicals; solid waste management; radioactive waste management; accidental waste management. Of course, these are just some of the major goals *Agenda 21* has intended to introduce in the policy of the signatory states starting 1992, in order to prevent situations of a global food crisis arising from a poor management of resources or the lack of measures for regeneration and protection of the environment.

In the *Agenda 2030*[9], another major document adopted by the UN member states, the signatory states aim to implement the concept of *"global governance"*, a collective management of the problems of poverty, malnutrition, underdevelopment and combating the waste born of the unsustainable pattern of the consumer economy, which creates global social inequalities[10].

Food security is also *closely linked to environmental security (by states taking the responsibility, internationally, to make conventions in the field of sustainable development, environmental protection, more precisely*). We can cite for example, the Convention on Climate Change/1994, the Convention on Biological Diversity[11]/1993, The World Heritage Convention/1975, The Ramsar Convention on Wetlands/1975, International Agreement on Tropical Forests/1997, Convention for the Protection of the Ozone Layer/1988, The United Nations Convention to Combat Desertification 1996, Johannesburg Convention on Sustainable Development and many more like these. All these international conventions are intended to ensure *a balance between the requirement of economic development* and the supply

[9] See https://www.un.org/sustainabledevelopment/development-agenda/, retrieved on 10 September 2019.

[10] *Ibidem.*

[11] See https://www.cbd.int/agro/soil.shtml, https://www.cbd.int/decision/cop/default.shtml?id=11037, https://www.cbd.int/doc/press/2018/pr-2018-11-29-cop14-en.pdf, https://www.cbd.int/doc/publications/cbd-sustain-en.pdf, retrieved on 5 September 2019.

of food for a constantly growing global population and, on the other hand, *the need for environmental protection*, biodiversity assurance, limitation and control of the extension of agricultural land, protection of forests and reduction of greenhouse gas emissions, restoration of the ozone layer etc.

We must also consider the Universal Declaration of Human Rights/1945[12], which, in art. 25, paragraph 1, expressly mentions *"the right of every person to food"*, within *"the right to an adequate standard of living"*.

The International Covenant on Economic, Social and Cultural Rights/1966[13] enshrined in art. 1, point 2, the sovereign right of the people, for their *"personal purposes"* (their national interest) to freely use their natural resources and it is provided that, *"in no case will any people be deprived of their livelihoods"*. Article 11 provides in the right of each person to an adequate standard of living, and *"the right to adequate nutrition for himself and his family"*, with the correlative obligation of States Parties to take measures for the effective realisation of this right. At the same time, art. 11 imposes on States Parties to recognise *"the right of every person to be free from hunger"* and consequently, the obligation to take measures to improve the methods of production, conservation and distribution of food, to improve the agrarian systems, by taking into consideration an equitable distribution of food resources, according to the needs of the countries, taking into account both the food-importing countries and the food-supplying countries.

In the United Nations Convention to Combat Desertification[14], for example, adopted by states under the auspices of the UN, since the preamble, it is recognised the negative impact of desertification and drought on sustainable development, *creating "major social problems such as poverty, malnutrition and poor health, lack of food security and other migration issues or the demographic dynamics"*[15]. *The need for international cooperation* to combat desertification and limit the effects of drought is emphasised, as well as *the need to open access to green technologies and to create new funds to help poor countries* in Africa but also countries in Transcaucasia and Central Asia affected by desertification and drought. States Parties to the Convention are aware of the link between desertification and environmental issues with global dimension, as well as the fact that, in meeting

[12] See https://www.un.org/en/universal-declaration-human-rights/, retrieved on 5 September 2019.
[13] See https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx, retrieved on 5 September 2019.
[14] *UN Convention to Combat Desertification in Those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa*, see https://www.unccd.int/, https://www.unccd.int/sites/default/files/relevant-links/2017-01/UNCCD_Convention_ENG_0.pdf, retrieved on 15 September 2019.
[15] *Ibidem.*

the objectives proposed by this Convention, they will also meet the objectives set out in the UN Framework Convention on Climate Change or The Convention on Biological Diversity or other Conventions for environmental protection.

In the July 2019 report issued by the World Resources Institute, on the global food crisis[16], a number of issues are addressed regarding: reducing growth in demand for food and other foodstuffs (which would involve measures to reduce food waste and wastage; switching to much healthier and sustainable diets; implications for poverty in restricting growth in demand for food). Another chapter of the report deals with the problem of increasing food production by avoiding the extension of agricultural land (assuming objectives such as: responding to the challenge of limiting the expansion of agricultural land; improving water and soil management; adapting to climate change); protecting and restoring natural ecosystems and limiting the change of agricultural land (including reforestation of abandoned, non-productive or virgin agricultural land; limiting the expansion of sowing land – cropland – to soils with low environmental costs); increasing the supply of fish (improving the management of wild fisheries; improving productivity and environmental performance regarding aquaculture); reducing greenhouse gas emissions; strategies for switching to smart agriculture and others[17].

The report shows that an increase in the global population from 7 billion in 2010 to 9.8 billion in 2050, accompanied by an increase in demand for food by over 50%, will lead to a demand for *"food much richer in intense resources"* such as meat and dairy, projected to increase by over 70% percent. Despite these increases in food demand, according to the report above, more than 800 million people are experiencing malnutrition or hunger. *States are obliged to quickly adopt solutions, measures, and policies to increase food production but under conditions of sustainability* (green economy, access to green technologies, smart agriculture) in ways that respect human well-being and the environment, at the same time[18]. At present, almost half of the world's *"vegetated land"* is used in world agriculture and this agricultural field generates a quarter of the annual greenhouse gas emissions, the report shows. In the future, it is essential for states to ensure *sustainable food security*, by avoiding the extension of agricultural land (which would affect other types of ecosystems), by practicing reforestation, avoiding deforestation, restoring

[16] World Resources Report, *Creating Sustainable Food Future. A Menu of Solutions to Feed Nearly 10 Billion People by 2050*, Final Report, July 2019, see https://www.wri.org/publication/creating-sustainable-food-future-final-report, retrieved on 15 September 2019.
[17] *Ibidem*.
[18] *Ibidem.*

damaged or abandoned land. Increasing productivity by increasing the efficiency of natural resources is an important step towards meeting the goals of food production and environmental protection, the authors of the above report show. In this respect, *the tendency to expand agricultural land must be avoided* in order to ensure feeding of the increased population, by 2050, to 9.8 billion people (which would mean the renunciation of forests, the extinction of species, the increase of the amount of greenhouse gases, the heating with over 2 degrees Celsius generated by the global development of the agricultural sector through this extension of land).

Another aspect considered in the report is *food demand management*, which requires states to pay more attention to *the development of food collection, sorting, recycling industries, within public policies to avoid food waste*, to which is added also a change in diet to plant products instead of animal products; improving women's access to education and health, especially in Africa to voluntarily accelerate the reduction of fertility. Another objective concerns the intensification of agriculture related to the need for the protection of natural ecosystems (a situation where *the location of agricultural lands extends* from one region to another, from temperate climate areas to tropical areas), resulting in *changes in the use of the land* that produces the increase of greenhouse gas emissions and biodiversity loss. Therefore, *a combination between intensified agriculture* (to avoid the extension of agricultural land to the detriment of other ecosystems) and the adoption by governments, *of legislation for the protection of forests, savannahs, other types of land, their exemption from agricultural extension* is considered in the report. The demand for meat-based nutrition is also projected to increase by 88% between 2010-2050, although it provides few proteins and calories. A reduction of meat consumption with 40% by 2050 would be required, given the general objective of changing the diet to a vegetable diet rich in protein and calories, to avoid the development of the animal breeding sector for consumption, with consequences in diminishing other ecosystems and increasing greenhouse gas emissions. Another important objective for the food security of the 9.8 billion people, in 2050, is *the reforestation and restoration of the lands, avoiding their desertification, as a way to combat climate change. It is vital to make the reforestation on a scale necessary to sustain a temperature rise not exceeding 1.5 degrees Celsius* (i.e., hundreds of millions of reforested hectares would be needed). This would be achieved if on a global scale there would be a move to intensive agriculture to replace the expansive one.

The doctrine brings into focus the concept of *"global environmental risk"*[19], defined as that type of environmental risk that does not know the borders,

[19] Marie-Claude Smouts, Dario Battistella, Pascal Vennesson, *Dictionnaire des relations internationales. Approches, Concepts, Doctrines,* Paris, Dalloz, 2006, p. 201.

whose damage no one can escape. If there is a global environmental risk, we can also discuss the concept of *"global food risk"*, defining it here as representing a specific type of risk born from a combination of several factors (demographic growth of the world population at 9.8 billion in 2050; insufficient agricultural land globally to provide food for this population; the need to protect other types of ecosystems and maintain biodiversity, thus preventing the extension of agricultural land; the need to ensure healthy and balanced nutrition, combating poverty and underdevelopment at the level of countries and regions; the need to implement green technologies and the need for reforestation to prevent climate change, ensure a breathable air and balance the terrestrial ecosystem). *The global food risk concerns the hazard coefficient for the environment and for a population of 9.8 billion people in 2050,* whose environment must satisfy the need for food and breathable air, under the following conditions: rising global temperatures and climate change; increasing urban pollution and pollution of soil and subsoil; increasing the level of waste discharges in nature, generated by a global consumer society; continually applying by states of the same pattern of consumption economy, meat-based food production and extensive agriculture, which have the effect of increasing greenhouse gas emissions; increasing the degree of urbanisation as well as the degree of global poverty; massive displacement of populations from region to region, from one country to another, from one continent to another, in search of satisfying the need for food (which the states of origin are no longer able to provide); lack of or insufficient industries for cleaning the environment, collecting and recycling discarded foods, recycling the plastic spilled in nature, using green energy and intelligent agriculture.

FOOD SECURITY AS PART OF NATIONAL SECURITY. NEW REGIONAL BODIES WITH COMPETENCIES IN THE FIELD OF FOOD SECURITY, IN THE 21ST CENTURY

Regarding the global food risk, the non-conventional threats will concern not only the governors, but also the national security of a country, that is, they will require the development of the skills of the armed forces to dimensions considered still, at present, to be *"economic"* (agriculture, management waste, food waste management, reforestation, use of green technologies in agriculture, reduction of greenhouse gas emissions). *Environmental security, as part of national security, will be rethought in strategic terms,* regarding *the protection of a country and its ability to respond to both national food risk and regional and global food risk.*

The ability of a country to respond *at the same time to several* food risks (local, regional, global), through strategies, policies, development of capabilities that fit the limitation, control and elimination of these asymmetric risks, *will lead to control over the effects generated* by these risks (migrations, massive, uncontrolled and sudden population movements, looking for food and fertile land to settle there; uncontrolled developments of situations that can lead to the effective suspension of regional agreements or the freedom of movement of persons in a common space, as it was the case with the Schengen agreement, suspended or inefficient, practically fallen, in 2015, in front of large movements of people from the Middle East and Africa to Western Europe).

If at EU level *we consider that, in the near future, the European Commissioner for Agriculture as well as the Commissioner for the Environment will have some of the most important functions* (considered strategic for the development of the EU as a green power or as a food power, in the context of population growth to 9.8 billion people in 2050), which can be supplemented or supported, in our opinion, by *a* ***European Food Crisis Management Office at EU level or associated EU countries*** (for the prevention and management of regional or global food risks targeting the EU, including in the form of population displacements from Central Asia, Transcaucasia, the Middle East or Africa), other initiatives may also be built in the future, *connecting the EU to the obligations undertaken by EU countries internationally, as UN member states* (*Agenda 21*, *Agenda 2030*, other international conventions on environmental protection), to provide an institutional framework *much improved* (in the field of sustainable development) *compared to the present one. Thus, in our opinion, the following future initiatives could be targeted:*

- Creating a *European Office for EU-wide waste management* (plastic waste, food waste, radioactive or chemical waste etc.);
- Creating a *European Office for the management of the fight against food waste, at EU-wide level* (with European sanctioning legislation for EU economic agents on non-collection, non-recycling discarded foods);
- Granting to *the EPPO/European Prosecutor special powers related to food and environmental crimes*, which concern crimes at EU or cross-border level, related to the *faulty management of agricultural lands* (their extension, instead of forestation), to the fertile land quality, to forestation, as a whole, *crimes related to sustainable development and its management at EU level*;
- Granting to EPPO/European Prosecutor special powers related to environmental crime (based on the adoption by the European Council and Parliament of compulsory waste management laws in the EU – qualifying as *"waste crimes"* at EU level the actions or inaction regarding collection, dumping, recycling, waste, at the level of EU economic agents and/or EU countries);
- Creating *a European Commissioner position on sustainable development at EU level*;
- Creating *an EU fund for the implementation of sustainable development to help developing countries* to provide intensive and intelligent agriculture and help for reforestation, in the global effort to restore ecosystems destroyed or affected by climate change and the advancement of desert areas;
- Creating *an EU fund for the implementation within the Union* of a green, intelligent agriculture, to support local and national projects for reforestation and restoration of the European forestry fund, in the effort to combat climate change;
- Creating *European legislation* on combating food waste, combating the use of plastic related to food trade and the production of packaging; the obligations of states and economic agents to remove plastic objects and to recycle them; the obligation of states to support and provide facilities for the waste recycling, plastic recycling industries; the obligation of states to replant abandoned, over-exploited agricultural land; the obligation of states to limit the extension of agricultural land, in favour of other ecosystems on the EU territory.

CONCLUSIONS

As we have shown in the present paper, the 21st century comes with a series of non-conventional threats, *which cannot be included in the classic concept* of national security or classical security risk. These are *non-conventional risks*, *a category in which we consider that enters also the environmental risk (local, national and global) as well as the food risk (local, regional, national, global)*, in the context of consolidating the aspects that indicate the *emergence of a global food crisis in the mid-21st century or even earlier* (according to the estimates of the specialist reports that indicate an increase of 9.8 billion people in 2050, hence the need to provide food, in parallel with the need to protect the environment and restore the ecosystems destroyed or degraded by human action).

National security as well as European security will have to be *redefined according to the parameters of food security*, in the context of the emergence

and the imposition on the global stage of the policy, *of new type of power, called by us the "food power"* , as power capable of designing commercial and economic policies of seizure and domination of the food markets (unprocessed commodities and processed foods) from entire regions (up to the formation of real spheres of influence, in a geopolitical sense, the food power attracting itself also the manifestation of a political power over the respective regions). *Ignoring such power* by strategies that address the types of threats to national and European security *would, in our opinion, lead to the creation and deepening of specific vulnerabilities in relation to rising food powers*, aware of the use and strategic advantages offered by exercising and assuming such a power, as an adaptation to the threats of the 21st century and to the specificity of this century.

BIBLIOGRAPHY

1. ***, *Agenda 21, United Nations Conference on Environment&Development*, Brasília, 3-14 June 1992, UN, *Sustainable Development*, https://sustainabledevelopment.un.org/content/documents/Agenda21.pdf
2. ***, *Agenda 2030*, https://www.un.org/sustainabledevelopment/development-agenda/
3. ***, Stratfor.com, 2 July 2012, *Developing Relations between Turkey and Europe*, quoted in Sorin Aparaschiva, *Turkey-Changes and Trends among the Political-Military Elites*, in the anthology of scientific communications *Turkey - from Kemal Ataturk to the EU*, coordinator Guven Gungor, Vasile Simileanu, International Scientific Paper Session, Geopolitica Club Cafe, Revista *Geopolitica*, București, 8-9 February 2013, Top Form, București, 2013.
4. ***, *UN Convention to Combat Desertification in Those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa*, https://www.unccd.int/, https://www.unccd.int/sites/default/files/relevant-links/2017-01/UNCCD_Convention_ENG_0.pdf
5. ***, World Resources Report, *Creating Sustainable Food Future. A Menu of Solutions to Feed Nearly 10 Billion People by 2050*, Final Report, July 2019, https://www.wri.org/publication/creating-sustainable-food-future-final-report
6. *Turkey – from Kemal Ataturk to the EU*, coordinator Guven Gungor, Vasile Simileanu, International Scientific Paper Session, Geopolitica Club Cafe, Revista *Geopolitica*, București, 8-9 February 2013, Top Form, București, 2013.
7. Viorel Roman, *Religiile, sursă de conflict*, Editura Academiei de *Înalte* Studii Militare, Bucureşti, 1992.
8. Vasile Simileanu, *Geopolitică* şi *centre de putere*, Editura Top Form, Bucureşti, 2010.
9. Marie-Claude Smouts, Dario Battistella, Pascal Vennesson, *Dictionnaire des relations internationales. Approches, Concepts, Doctrines*, Dalloz, Paris, 2006.

WEBOGRAPHY

1. https://www.cbd.int/agro/soil.shtml
2. https://www.cbd.int/decision/cop/default.shtml?id=11037
3. https://www.cbd.int/doc/press/2018/pr-2018-11-29-cop14-en.pdf
4. https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx
5. https://www.cbd.int/doc/publications/cbd-sustain-en.pdf
6. https://www.un.org/en/universal-declaration-human-rights/

INTELLIGENCE EDUCATION – STRATEGIC INNOVATION –

Dan COLESNIUC, PhD
Defence Intelligence General Directorate

Decision-making in the current operational environment, characterised by complexity, dynamism and unpredictability, requires continuous adjustment and optimisation of training and education processes in the military training field.

Romania's affiliation to international organisations and alliances involves seamless strategic approach, from the conceptual point of view, to implementing common standards, as outcomes of best practices specific to the defence intelligence field. This approach requires future military leaders' training in an interdisciplinary and multicultural cognitive space. Thus, continuous innovation in the educational field has direct contribution to projecting and developing early warning systems in order to avoid strategic surprise.

Virtualising the battlefield replaces the hierarchic-type thinking with the network thinking, a reflexive collaborative approach where working tools specific to the intelligence activity must be characterised by adaptability and flexibility for timely decision-making.

Keywords: education, interdisciplinarity, multiculturalism, strategic decision, intelligence.

Motto:
"You must have the courage to give up on who you are to become who you deserve to be".
Albert Einstein

EDUCATIONAL INTEROPERABILITY IN THE CONTEXT OF GLOBAL CHALLENGES

Education is, by far, the key public project of Romania from the perspective of its integration into political-military and economic structures, European and Euro-Atlantic ones. The historical stake is the integration in a system of values that will allow the continuous and sustainable development of Romania, under the conditions generated by its membership of NATO, since 29 March 2004, as well as of the European Union, since 1 January 2007.

From this perspective, the complex and long-term focus on the profound transformation of education, on all levels, is the essential condition for the success of European Romania.

The need for profound transformation is the result of improper structural design, the dominant focus on the transmission of knowledge, to the detriment of the formation of skills through the development of transferable skills and attitudes based on values.

This mode of operation has allowed for the cultivation of the most acute, decisive and specific reactive behaviour at large. This kind of reactive attitude can be characterised by minimal receptivity to the complex processes defined by the profound adaptive changes, similar systemic approaches from the perspective of different realities and a limited structural understanding regarding the rapid construction of value-added elements, characterised by flexibility, adaptability, sustainability and high-learning capacity.

One of the reasons for the lack of a proactive attitude is determined by the excessive focus of the education system on knowledge, which, by definition, becomes more perishable in relation to the skills and attitudes acquired in the educational process. Thus, of the three verbs that define the model of human development through education, *"to know"*, corresponding to the accumulation of knowledge, *"to do"*, associated with the practice and development of competences and *"to be"* regarding the process of attitudes formation, the most stable

is the third one, because the cultivation of attitudes is directly related to the development of long-term personal value systems.

In this context, the educational transformation becomes a process of profound adaptive change, in which its approach requires a dominant position of reflection and action in the leadership concept.

The end of the Cold War has led to a reconsideration of the security concept beyond the traditional approaches, in terms of militarisation and the central state, specific to the bipolar era. The universalist approach to security relating to the human community, with the same common global concerns, determines a shift in the focus from that on the state security concept to that on the individual.

Today, the idea of security must be viewed in a broad sense, encompassing economic development, social justice, environmental protection, democratisation, disarmament, rule of law and respect for human rights.

New transnational entities, such as terrorist and organised crime networks, are diversifying in terms of how they are organised and how they operate, increasing their power of action to achieve their own interests.

From a decision-making perspective, the causes of the non-military roots of instability coexist with the military implications and, therefore, it is necessary to create a common framework for cooperative solutions with multiple actors, governments, NGOs, international organisations, agencies and international coalitions.

In a non-linear operational space, defined by volatility, uncertainty, complexity and ambiguity, however, participatory thinking and a holistic understanding in the dynamics of collecting, analysing and making critical decisions in real time become increasingly relevant.

Collective knowledge in the allied environment, such as lessons learned and direct participation in experience exchanges and practical activities, is a priority of educational processes, of promoting cooperation with NATO and non-NATO members. Such cognitive dissemination is based on bi- and multilateral training, exercises and common topics of scientific research and continuous development, as determining factors for generating influence and accomplishing the tasks undertaken in the allied environment.

DYNAMICS OF THE ADAPTIVE TRANSFORMATION OF EDUCATION IN THE FIELD OF DEFENCE INTELLIGENCE

The increasingly dynamic characteristics of the operational environment represent a direct and immediate challenge for the traditional military education system. The classical methods of preparation have followed over time the development of the skills necessary for success, in a symmetrical environment, characterised by centralised decision-making processes in a linear battle scenario.

Adaptive change, however, generates discomfort because, by its very nature, it causes significant losses for those who face this change: status, beliefs, attitudes and habits. Exercising effective leadership at this stage creates the favourable environment for rhetoric and re-examination of one's own beliefs and value systems.

The spectrum of current and prospective military activities, peacekeeping or fighting, requires the development of skills of relational training, confidence building, communication and collaboration with various socio-human entities, situational understanding, multicultural and interdisciplinary interaction in complex environments.

Through education, critical thinking and analytical thinking skills are developed, which are temporary processes. If the training process provides the right or wrong answers that allow the measurement of the immediate preparation progress, the education is incremental when confronted with the unpredictability of changing the operational environment.

Furthermore, the new military capabilities are amplified by the knowledge multiplier in a confrontation space characterised by knowledge-based operations.

Therefore, the competencies by which the sources of information are accessed, evaluated and used represent fundamental skills in the information society, where the demands for new knowledge are determined by new challenges with a high degree of complexity.

Thus, knowledge management, as an internal process of virtual distribution of information within an organisation or inter-agency, is an essential added value in supporting decision-makers at the strategic level. This synergy is reinforced with the result of competitive intelligence analyses on some impact factors (global phenomena, threats, crises, technological trends etc.) in the activity of transformational adaptation and strategic positioning of the organisation.

The implementation of a process thinking, structured on dependent or independent activities, which bring together people and resources in a transparent way, allows the development, refinement and quantification of timely reaching the operational objectives. Thus, the efficiency of the temporary component, the decisional basis, the identification of repeatable models in similar circumstances and the dynamics of transferable knowledge increase.

The relations between allied and partner nations, particularly at the level of military experts interacting with those in the civil security and public order sector, become critical in a hybrid confrontation environment, in which knowledge-based operations will be determined by military power, civilian capabilities and direct interaction with the host nation. This strategic situational awareness generates new types of conceptual relationships between strategy, technology and the security space in the informational age.

Therefore, continuous professional and personal development of the specialists is required in order to improve the flexibility of critical thinking, to increase the management and leadership capabilities. Moreover, it is also required from the perspective of implementing adaptive technologies specific to the informational age, in collaborative and network terms, against the background of digital transformation of the company and the *"cybernetisation"* of the operational space.

"Top-down"-type hierarchical teaching-learning methods, platform-centred, location-dependent, simultaneous and direct interaction of the teacher with a high number of students, as well as temporary restrictions, must be gradually replaced by a customised model, focused on the bilingual student-teacher approach, based on new online technologies that provide content on demand.

These new technologies, implemented in IE-learning systems (Intelligence Education-learning), aim at clearly and explicitly define the problem, logically develop the argumentation and receive an answer that reflects the dynamic understanding of an event's or phenomenon's evolution. The miniaturisation of terminals or devices offers, through their friendly interfaces, a quick availability to install and configure the necessary software applications, which represent a new paradigm of network-centred warfare. Additionally, IE-learning systems must contain an operational component of serious games, reflecting situational awareness, role-playing, interpreting, adopting strategies, and obtaining authorised feedback from experts. Moreover, the implementation of war games applications will contribute to a better understanding of the cultural-cognitive aspects and a better coordination in the allocation of resources, a priori to the dislocation of forces in the confrontation, tactical-operative and strategic space.

To conclude, government education systems represent this millennium's challenge for all the world states, regardless of their geographical positioning or their level of socio-political and economic development. This approach is generated by the dynamics of the transformations in the human values system, against the background of the technical-scientific revolution registered worldwide, in all activity fields.

All these aspects and other similar initiatives developed within the military education system represent key aspects in profound analysis of the critical interdependencies between the educational strategies, capabilities and technologies necessary to ensure the influence and effect of the decisions taken at all hierarchical levels.

Continuing the sustainable development of a multilateral interconnection model in the educational field, both from a curricular point of view and of the technologies used, represents a level of ambition that will generate new competencies against the operational-strategic challenges of the information age.

The recruitment, training and modelling of active personnel, able to act in a complex, dynamic and extremely volatile environment, prepared to fulfil a wide spectrum of tactical, operational and strategic missions, must represent the key objectives of the training and continuous professional development process of the Ministry of National Defence specialists. Interoperability in the tactical, operational and strategic field will be determined by the creation of an intellectual-educational interoperability regarding the semantic understanding of the specific concepts, which will help to build confidence in the allied environment.

BIBLIOGRAPHY

1. ***, *Strategia de dezvoltarea a învăţământului militar şi formării continue 2018-2030*, project, Human Resource Management Directorate, Bucureşti, 2018.
2. Dan Colesniuc, *Foster Education by Technology*, 14th International Conference, *Learning and Software for Education*, Bucharest, 2018.
3. Norman Friedman, *Thank You for Being Late. An Optimist's Guide to Thriving in the Age of Acceleration*, Penguin Random House, UK, 2017.
4. Dov Seidman, *How: Why HOW We Do Anything Means Everything*, New York Times, 2011.
5. www.nato.int.
6. www.nato.int/strategic-concept.

THE IMPLICATIONS OF ILLEGAL MIGRATION AND REFUGEES ON EUROPEAN SECURITY

Alexandru PETERCĂ

280th Mechanised Infantry Battalion "Captain Valter Mărăcineanu", Focșani

The crisis that started in 2015 revealed a deficient European migration system. The leading bodies of the European Union did not foresee such an event, being put in a position to react to the reality of the events in progress. Creating a system of compulsory quotas for asylum seekers, increasing security at internal and external borders, as well as managing the control of immigrants with illegal status are just some of the responses to this phenomenon.

Keywords: crisis, refugees, migration to Europe, organised cross-border crime, immigrants.

INTRODUCTION

Migration is one of the oldest phenomena recorded in the history of mankind. Over time, it has manifested with a different intensity and developed new forms, but now, in the first part of the 21st century, it seems that it has reached the highest threshold since the end of World War II.

The reasons behind the people's choice to migrate from one place to another are diverse, but a brief look at the history of the phenomenon reveals that the main impetus is the existence of circumstances that aggravate the living conditions and in which the vicissitudes of life are greatly amplified. Man's desire to meet one of his primary needs, namely personal security, is the central vector around the decision that has led mankind to leave their homeland and move to places where high standards of living creates the impression that needs can be reached way easier than in the original locations.

Here, with the passage of time, with a much clearer picture on the people's borders and with the creation of widely detailed legislative frameworks – keeping in mind the same human desire to achieve personal security (but not only) and the same circumstances that prevent it – the phenomenon of migration has developed a new connotation, namely illegal migration. Illegal migration is a way of materialising organised crime that has repercussions on the security, economy and social situation of the countries transited by migrants or refugees, as well as of the states that are the final destination.

In order to thoroughly understand the migration phenomenon, it is necessary to record two key terms: *"migrant"* and *"refugee"*.

According to the UN, the migrant is considered to be the person who, during a minimum of 12 months, has resided in a country other than his native one, regardless of the causes and the means used for it[1]. Most of the times the motivations of the migrant people are to obtain better living conditions and higher quality education than those available. The legality criteria divide the migrants in two categories: with legal status (the individual who obtains access to the territory of another country and who remains in that state in compliance with the rules of his admission);

[1] David Bartram, Maritsa V. Poros, Pierre Monforte, *Key Concepts in Migration*, SAGE Publications Ltd., 2014, pp. 4-8.

with illegal status (migrant who has crossed the border to another state without having legal status in the respective country and violating the access criteria)[2].

Another element to be considered is forced migration. It was introduced by the International Organisation for Migration by adding a new parameter to the equation – constraint. This type of migration refers to people who have been determined to migrate by coercive reasons, such as the existence of life-threatening hazards, regardless of whether they are natural or not (famine; chemical, biological, ecological, radiological, nuclear disasters; refugees)[3]. In this regard, it is marked the transition from migrants whose motive is the search for a higher quality of life to those looking for normal living conditions.

The Geneva Convention of 1951 addresses the status of refugees and defines as a refugee any person *"(2) owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable, or owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it"*[4]. Having as motivating factors to leave the hotbeds of armed conflict and the threats to their fundamental rights, the refugees have the motto to obtain the conditions of a quiet life.

GEOPOLITICAL CONTEXT

As mentioned above, the European Union states are currently facing the biggest migration crisis since 1945. Its predominant source is represented by the armed conflicts, persecutions and general climate of political and military instability in the extended neighbourhood of the European space.

2015 is the year when Europe was the destination of over 1 million refugees and immigrants, thus unexpectedly marking an unprecedented event. Most of these people come from states with a high degree of instability in Asia, Africa and the Middle East. For the most part, these countries have either been or are currently considered conflict zones where terrorist cells or organised crime groups exert enormous pressures on the citizens.

[2] Alexandra Sarcinschi, *Considerații teoretice în sprijinul înțelegerii provocării de securitate constituită de criza europeană a refugiaților și migranților ilegali*, in *Gândirea Militară Românească*, no. 3/2018, see https://gmr.mapn.ro/pages/view/80, retrieved on 5 August 2019.

[3] Richard Perruchoud, Jillyanne Redpath-Cross (coordinators), *"Forced Migration"*, in International Organisation for Migration Glossary on Migration, 2nd Edition, 2011, see https://www.west-info.eu/files/iom.pdf, retrieved on 3 August 2019.

[4] *Convenția privind statutul refugiaților*, see https://www.unhcr.org/3b66c2aa10, retrieved on 3 August 2019.

Concomitant with this crisis, at European level, it can be noticed the highest intensity of terrorist attacks in the last two decades. Moreover, the United Kingdom has decided to leave the EU and it is increasingly difficult for the diplomatic tools to maintain the fragile balance between the EU enlargement, the preservation of internal stability and the perpetuation of its elementary rules, and the execution of controls at most of the internal borders of the EU states almost temporarily suppress the concept behind the Schengen area[5].

The problems listed above and the migration phenomenon are in an obvious connection, and the way in which the hegemonies in the area of interest, as well as the institutions or organisations empowered and responsible in this regard react are cardinal parameters in solving this crisis.

The massive flows of immigrants have strongly affected the balance of the European Union, so that among its members there have been many tensions, contradictory positions at extremes and even threats of leaving the alliance, one of them being in the process of materialisation (see *"Brexit"*). The attacks in which migrants were involved, the violence out of gender reasons and the Brexit process are some of the reasons that determined the Europeans' reluctance to the idea of compulsory refugee quotas[6].

At present there is a downward trend compared to 2015, when illegal migration saw a record number. However, a series of fluctuations continued both in 2018 and in the first half of 2019, an aspect that highlights the need for sustained measures, as well as a reaction system that is able to adapt to the changing circumstances.

At the level of the central-Mediterranean area, the phenomenon of illegal migration remains low, the year 2018 marking for the Italian state a downward trend of arrivals (by 80% less) compared to the previous year, a trend that continued in 2019. Despite the fact that over 50% of the migrants in 2018 were of Lebanese origin, the coast guard of Libya has intercepted and/or saved an impressive number of people along the sea (about 15,000), these being from countries such as Eritrea, Sudan or Niger. Tunisia in its turn became a major starting point to the Italian state, and towards the end of 2018, Malta was facing an upward trend of migration arrivals. As for the western-Mediterranean route, the situation is slightly different. 2018 saw an increase in the number of arrivals compared to the previous year, Spain obtaining a percentage of 131% of entries compared to 2017, a trend that continued in 2019. Most people who chose this route have Moroccan, Algerian origin or come from other western states from African continent such as Guinea,

[5] Dan Fifoiu, *Migrația ilegală – o privire din surse deschise*, 2017, see https://intelligence.sri.ro/migratia-ilegala-o-privire-din-surse-deschise/, retrieved on 5 August 2019.

[6] *Migrația ilegală – riscuri* și *oportunități*, 2017, see http://romaniasmart.ro/2017/01/03/migratia-ilegala-riscuri-si-oportunitati/, retrieved on 5 August 2019.

Ivory Coast, Mali, Gambia. Similar to the western route, the eastern route marked an upward trend in 2018, with Greece receiving 30% more migrants in 2019. All these fluctuations have produced enormous pressure on the Aegean islands, but especially on the land border between the Turkish and Greek states. The frustration of the Greek state is all the more pronounced as the number of returns to Turkey is insignificant, having no impact in trying to reduce these pressures and in the fight against the groups dealing with illegal migration. The statistics of the last 18 months reveal that Afghan citizens are the most who chose these islands as their destination, and as regards the border between Greece and Turkey, it has been mostly passed by Turkish migrants. For the route that passes from the Serbian state to the Bosnian state, the previous year reported four times more illegal crossings than in the previous one. Earlier this year, Bosnia and Herzegovina noted around 24,000 immigrants with irregular status, most of them using this route. However, it is important to note that with the removal of the visa-free travel system of Iranians by Serbia, the number of people using this route began to decline[7].

Looking at these statistics, the European community seems to be facing strong influences of ethnicity, culture and religion which, due to discrepancies in mentalities, may lead to an increased risk of internal conflicts in society.

RISKS AND CHALLENGES

The crisis caused by the waves of arrivals has led to a series of risks and threats for European countries. The migration phenomenon is characterised by a high complexity and a wide range of variables that must be taken into account. Of these we mention the origin of refugees or immigrants, their number relative to a certain period of time, the extent to which the receiving country can manage the large inflows of arrivals or the reaction of the local population to this massive volume of immigrants.

The states that in the past have sympathised with, or even promoted for a long time, the idea of receiving migrants, now have the largest demographic imbalances. These strategies have in time led to the accumulation of massive shares of immigrants in the same location, which has led to the formation of economic, social or ethnic cleavages between them and the indigenous population. Although they have been found in the host country for several generations, often the importing communities have not found solutions by which foreigners adopt and adapt to the local particularities while preserving their values, traditions

[7] *Raport privind progresele* înregistrate în *punerea* în *aplicare a Agendei europene privind migrația,* Brussels, see https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52018DC0301, retrieved on 4 August 2019.

and culture. The neglect of the host population and the reluctance to adapt of those who have come have led to the formation of different communities and, in some cases, it has led to the situation where the two groups, although they are on the same space, marginalise each other, each seeking not to alter their own values and habits with those of the neighbours.

If a significant number of immigrants of the same origin are pooled in certain communities, social problems may become more difficult to detect. Although in the first instance the image of an efficient integration is formed, in fact, this merger determines deficiencies in the accommodation process in the host society. From the desire to live according to one's own rules and not to those of the adoptive society, a parallel can be drawn to the creation of national enclaves based on religious or ethnic reasons[8].

Unquestionably, in this context, there are accusations from both sides, which can sometimes be in the form of racist, xenophobic or physical altercations. All these cultural, economic, religious, and social differences will create frustrations until the limit of sustainability is reached. From that moment until the formation of radical, extremist or terrorist organisations, there is only one step.

At the social level, the host states face the challenge given the promotion of subversive conceptions and ideologies that incite the violation of laws. It is also possible that the locals, especially those in the vicinity of the borders, will be attracted to activities of a criminal nature thus increasing the actions specific to organised crime. The easy access to the internet for anyone and the use of the information environment as a means of spreading extremist propaganda create the risk of self-radicalisation. Getting in touch with already radicalised individuals and/or frustrations due to unfulfilled expectations from the host state are potential factors for some migrants to join extremist movements. At the same time, it should be borne in mind that, with the arrival waves, the risk of proliferation of contagious exotic diseases is high.

At the economic level, each state spends an important part of its own budget to provide refugees with medical facilities, accommodation, food and education during transit or during their integration. European Union projects to mitigate the effects of migration require for each member to contribute significant amounts of money. Moreover, independent efforts to increase border security measures (for example fence construction) must be taken into account. The economy of the countries of transit or final destination is also affected by the cheap labour force

[8] *Migraţia ilegală – riscuri* şi *oportunităţi*, 2017, see http://romaniasmart.ro/2017/01/03/migratia-ilegala-riscuri-si-oportunitati/, retrieved on 6 August 2019.

generated by the arrival waves. This has an upward impact on the unemployment rate among the local population and raises frustrations and tensions between the two parties. It should also be mentioned that some companies will hire migrants without providing them with a legal framework, which directly damages the host state and which may lead to violations of rights (prolonged work schedules, money remuneration lower than the established minimum wage by law, eventually and without providing medical services - so-called *"paid under the table"*)[9].

At the security level, migration offers the chance to capitalise on the channels of illegal migration and provides opportunities to members of terrorist networks or supporters of radical ideologies to infiltrate the European space more easily and to incite violence, terrorist acts or other fraudulent actions.

The increase in terrorist risk is one of the most debated problems associated with migration. The existence of evidence regarding the involvement of immigrants in carrying out attacks has greatly increased the reluctance of European society to the migration phenomenon, and some states have even implemented the maximum level of alert regarding terrorism.

MEASURES OF THE EUROPEAN COMMUNITY

At the last meeting on the migration topic, on 28 June 2018, the European Council reiterated that a comprehensive approach to migration is based on a functional policy, which combines the efficiency of the control of the EU's external borders with the intensification of external and internal actions, respecting the norms and values of the union. This is not a challenge for a single EU state, but it concerns the whole European community. At this meeting, new measures have been implemented to reduce illegal migration and to eliminate the chance of new waves of uncontrollable migrants like the one of 2015.

Following the implementation of the directions established in 2015 by the EU Migration Agenda (strengthening and improving security at the external borders, in particular by improving border procedures, as well as saving human lives; diminishing the factors leading to illegal migration, emphasising the efficiency of putting into practice return policies and addressing the basic considerations underlying the issues of third countries; reviewing and strengthening the common asylum and migration policy; formulating a new migration policy addressing the Union challenges and demographic future risks[10]), there have been impressive

[9] Georgiana Chirilă, *Migrația ilegală sau cum se importă riscurile de securitate*, 2016, see https://intelligence.sri.ro/migratia-ilegala-sau-cum-se-importa-riscurile-de-securitate/, retrieved on 6 August 2019.

[10] *Politicile UE* în *domeniul migrației* și *azilului*, see https://www.mae.ro/node/35902, retrieved on 2 August 2019.

results such as the decrease in arrivals on the Eastern and Central routes by 97% and 80% respectively, catching over 2,000 migrant traffickers and removing over 375 boats[11], as well as saving over 690,000 people at sea, of whom over 400,000 in 2015 and 2016 alone.

Regarding the central transit route, the European Council has supplemented the measures by agreeing on the multiplication of actions to prevent the migrants trafficking networks, the sustained support of the states considered in the first line (for example Italy), the increase of the cooperation with the transitional and origin states, as well as by intensifying voluntary relocation.

As for the Eastern route, European leaders have emphasised the observance and application of the EU-Turkey Agreement[12], the ban on arrivals from Turkey and the stopping of flows. Moreover, it was approved to grant the second tranche of money in support of refugees hosted by Turkey.

It was also agreed on intensifying the attempts to prevent illegal migration along the western route, where there is an upward trend in this regard. This calls for the efforts of both EU countries and the countries of transition or of origin, especially the state of Morocco.

Regarding the people rescued from the sea, the concept of the regional landing platforms was approved for development, through which the reliable and rapid distinction between refugees and economic migrants could be made.

The European Council members have jointly decided to set up controlled centres, by the Member States on a voluntary basis, through which the rescued persons from the territory of the EU will be efficiently processed and through which the safe distinction between the irregular migrants, those who will be returned, and those who are in real need of international protection will be achieved.

Another measure aimed at intensifying cooperation with Africa, both by increasing funding for development and by creating a new framework to promote an upward trend in the sense of investments of private organisations in this region. In addition, the establishment of a tool for the management of external migration has been added to the long-term budget list.

[11] *EU and Migration Crisis*, 2017, see http://publications.europa.eu/webpub/com/factsheets/migration-crisis/ro/, retrieved on 8 August 2019.

[12] The 2016 EU-Turkey agreement underlines the prohibition of illegal migration on the eastern route, combating human trafficking organisations and providing humanitarian support for the 2.5 million Syrian refugees in the Turkish state by financing 3 billion euros for various projects for their benefit (2 billion are covered by the EU budget, and the difference comes from the contributions of the members).

The mandate of the European Border and Coast Guard Agency[13] (established on 6 October 2016) has been extended, and the concepts of maintaining effective control of the external borders and returning illegal immigrants have been recalled.

Regarding the internal context, each state must take all the measures required to prevent the secondary movements of those seeking asylum and to form an effective cooperation between the members of the Union for this purpose.

The last discussions of the Brussels meeting of 28 June 2018 referred to the principles of asylum and marked the progress towards the completion of five of the seven legislative proposals of the European Commission in the package on the Common European Asylum System launched in 2016 and 2017[14].

CONCLUSIONS

The continuity of the existence of regions with a high degree of economic, military and political instability, which presents a great potential for migration, the low living standards in which large populations from several external areas live, correlated with the ingenuity of the cross-border criminal groups, represent the cardinal parameters that support and encourage the preservation of the illegal migration phenomenon at a high level.

The increase in the number of arrivals on the European states' territory has led to the increase in the pressures, regardless of the level at which they acted (social, demographic, cultural, religious, administrative, economic), on all the transited states and, to the same extent, to a significant security risk. Moreover, the colossal number of migrants *"waiting"* at the EU's external borders keeps *"in business"* the cross-border organised crime networks, further encouraging these groups in illegal activities.

In addition, most transitional states are facing a crisis that goes beyond their capacity to effectively control the situation. Therefore, they are under the pressure generated by the fear of becoming a blocking migrants area for an indefinite period.

However, we must not forget that, although this crisis has had a multitude of negative effects, the waves of migrants offer a refresher of the workforce, especially for the states that are facing the demographic aging phenomenon and also create the ideal framework for innovative management initiatives.

[13] One aspect was the mobilisation of over 1,550 agents in support of the countries on the EU's external borders.

[14] Dublin Regulation laying down the criteria and mechanisms for determining the Member State responsible for examining an application for international protection; Regulation establishing the European Union Agency for Asylum; Regulation laying down EURODAC (biometric database); Regulation laying down a common procedure for international protection in the EU (replacing the Asylum Procedures Directive); Regulation on the qualification of third-country nationals or persons without nationality as beneficiaries of international protection (replacing the Qualifications Directive); revision of the Reception Directive Conditions for the international protection applicants; establishing the legal framework at European level in the field of external relocation.

The European Union's ability to cooperate with partners from third countries will be crucial to ensure response to this crisis and to jointly control the challenges and capitalise on the opportunities that arise. Also, within the EU, the existence of deficiencies in the coordination between the states and the agencies that must identify joint solutions to the challenges and risks related to the illegal migration phenomenon, can perpetuate security problems, affecting both the regional and national level.

BIBLIOGRAPHY

1. ***, *Convenţia privind statutul refugiaţilor*, 28.07.1951, http://www.unhcr.org/ ro/wp-content/uploads/sites/23/2016/12/1951_Convention_ROM.pdf
2. ***, *Migraţia ilegală – riscuri* şi *oportunităţi*, 2017, http://romaniasmart.ro/2017/01/03/migratia-ilegala-riscuri-si-oportunitati/
3. ***, *Migrația ilegală sau cum se importă riscurile de securitate,* https://intelligence.sri.ro/migratia-ilegala-sau-cum-se-importa-riscurile-de-securitate/
4. ***, *Politicile UE în domeniul migraţiei şi azilului*, https://www.mae.ro/node/35902
5. ***, *Raport privind progresele înregistrate în punerea în aplicare a Agendei europene privind migrația,* Brussels, https://eur-ex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52018DC0301
6. ***, *EU and Migration Crisis*, 2017, http://publications.europa.eu/webpub/com/factsheets/migration-crisis/ro/
7. David Bartram, Maritsa V. Poros, Pierre Monforte, *Key Concepts in Migration,* SAGE Publications Ltd., 2014.
8. Dan Fifoiu, *Migraţia ilegală – o privire din surse deschise*, 2017, https://intelligence.sri.ro/migratia-ilegala-o-privire-din-surse-deschise/
9. Richard Perruchoud, Jillyanne Redpath-Cross (coordinators), *Forced Migration,* in *International Organization for Migration Glossary on Migration*, 2nd Edition, 2011, https://www.west-info.eu/files/iom.pdf
10. Alexandra Sarcinschi, *Considerații teoretice în sprijinul înțelegerii provocării de securitate constituită de criza europeană a refugiaților și migranților ilegali*, in *Gândirea Militară Românească*, no. 3/2018, https://gmr.mapn.ro/pages/view/80
11. Alexandra Sarcinschi, *Migrație și securitate*, Editura Universității Naționale de Apărare *"Carol I"*, București, https://cssas.unap.ro/ro/pdf_studii/migratie_si_securitate.pdf

CYBER SECURITY
– THE GREAT CHALLENGE OF THE 21ST CENTURY –

Petru-Viorel ENE, PhD
Department for Parliament Liaison and Personnel Welfare, Ministry of National Defence

Nowadays cyber security is essential for individuals, companies, governments and nations as whole. As our society and our economy become more and more digital, the technologies used are replaced, updated and constantly modified. In response, cybercriminals are paying more attention to how they are using technology to commit malicious activities on digital networks. In this context, cyberspace, which is constantly changing, generates not only development opportunities but also risks and challenges. All these vulnerabilities make cyber security a major priority for all the entities.

World governments have invested significant amounts of money to defend their own data because any initial investment is lower than the funds required to recover from a cyber-attack and, on the other hand, a cyber security incident in one country may well have an impact across national borders. Therefore, what steps should we follow?

Keywords: network, security, threat, vulnerability, digitalisation.

INTRODUCTION

When the Internet started expanding, many optimistic voices predicted its benefits, which are considered absolutely fabulous if we are talking about the economic sector and the amount of information to which we have access.

At the European level, we are witnessing the need for a more secure cyberspace and therefore, we have to support the efforts to define the norms of behaviour in cyberspace to which every stakeholder should adhere. In this regard, the European citizens have to respect their civil duties, social responsibilities and laws online, so states should abide by existing norms and laws. Developing cyber security capacity is a responsibility for both private and public sectors. Moreover, the civil society must help building a safe cyberspace.

At the same time, the expansion of cyberspace, the increased global connectivity and the cyberspace impact on the physical world have generated many challenges. On this matter, all the states should cooperate because a cyber security incident in one country may well have an impact across national borders. Furthermore, service providers often operate across EU countries, especially telecom companies and internet service providers. It is cumbersome for these providers to have to adapt their systems to different national requirements.

An important pre-condition for a free, open and secure Internet with all its benefits to societies worldwide, is to maintain the permanent cooperation of the relevant stakeholders[1]. This is a priority for the European community as evidenced by the measures taken by the European Defence Agency (EDA) that is developing cyber defence capabilities and technologies in order to improve cyber defence training and civilian-military dialogue as a contribution to the co-ordination between all actors at EU level.

In recent years a number of European Member States have recognized the need for preventing cyber security incidents and they started up, for example, voluntary or mandatory incident reporting schemes to create more transparency about cyber security incidents. In these countries the focus has often been on the vital infrastructure for the digital society, the electronic communication networks and services[2].

[1] Jochen Rehrl, *Handbook for Decision Makers – The Common Security and Defence Policy of the European Union*, Imprimerie Centrale, Luxembourg, 2017, p. 164.
[2] See https://www.enisa.europa.eu/topics/incident-reporting?tab=details, retrieved on 23.08.2019.

As our society and our economy have become more and more digital, our European answer starts with education and skills for everybody. We need better cyber security, not only to protect our data and privacy, but also to prevent the misuse or damage of our networks and systems. In this framework, not only states but everyone has a key role in keeping the internet safe[3].

We have already experienced the impact of the Internet in this new digital era and we can say without a shadow of a doubt that the consequences can be devastating with great costs like industrial accidents and natural disasters. So, we must address this issue with utmost seriousness and to involve states, private sector and citizens.

BENEATH THE SURFACE OF A CYBER ATTACK

Over the past two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too[4].

In recent years we have seen that while the digital world brings enormous benefits, cyber threats becomes more frequent, complex and destructive. The EU and its Member States are increasingly faced with non-conventional threats that are global and transboundary and have a strong disruptive effect on the EU. Among these threats the spread of cyberattacks capable of disrupting critical infrastructures represent a major issue.

Some of the defining characteristics of these non-conventional threats is that they: are not executed, nor can they be tackled, exclusively by military means, and they do not qualify as an armed attack in the sense of Article 5 of the NATO

[3] See https://www.enisa.europa.eu/media/multimedia/videos/cybersecurity-is-a-shared-responsibility-european-cyber-security-month-2018, retrieved on 23.08.2019.

[4] See https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, retrieved on 23.08.2019.

Treaty[5]; ignore borders; target individuals or companies rather than states directly; have major psychological and economic impacts and require strong intelligence capabilities for their detection, prevention and attribution.

These characteristics mean that purely national efforts have a limited impact – as do measures taken within the traditional boundaries of security and defence. Against this backdrop, the EU is in a unique position to foster the necessary deeper synergies between internal and external security, and defence policies and instruments[6].

EU but also NATO members have taken important steps in cyber defence over the past decade. The need to strengthen capabilities and to cooperate to defend against cyber-attacks was first acknowledged by Allied leaders at their 2002 summit meeting in Prague[7]. Since then, cyber security has become an increasingly important focus on every country agenda.

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for transparency, accountability and security is becoming more and more prominent. The latter issues should be a priority for all states and should guide their cyber security policy in fighting with all threats that appear.

Cyber security threats are released by hostile entities, state or non-state actors, over the information infrastructures of strategic interest of public institutions and companies. In this category we also include the cyber-attacks developed by the criminal groups. All these attacks will directly affect the national security of a country[8].

In order to have an overview of this phenomenon, it is important to run a brief analysis of the cyber threats and their impact, first in Romania, and after that worldwide. In this respect, we mention the study carried out by Bitdefender, the

[5] The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security, https://www.nato.int/cps/en/natolive/official_texts_17120.htm, retrieved on 24.08.2019.

[6] European Political Strategy Centre, *The Defence-Security Nexus – Towards an EU Collective Security*, 2017.

[7] See https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm, retrieved on 24.08.2019.

[8] *Strategia națională de apărare a* țării *pentru perioada 2015-2019*, București, 2015, p. 14.

biggest cyber security and antivirus software leader, protecting over 500 million systems in more than 150 countries.

According to it, Romania is the country most affected by *Scranos*, a malicious rootkit driver that steals user passwords and account payment methods stored in a victim's browser. Bitdefender alerted the authority issuing the digital certificate that masked the *Scranos* threat about its compromised and illicit use, and the driver's digital signature was afterwards revoked for solid suspicions of fraudulent activity. Originating in China, *Scranos* was discovered in April, when it spread aggressively in Europe and United States, contaminating Windows and Android devices and accessing the victims' personal data[9].

Kaspersky Lab, another huge software and hardware security provider, informs us that Romania occupies the sixth position regarding the attack from mobile ransomware. We observe that Romania is an attractive country for cyber-crimes and the mobile threats has been constantly evolving not only in terms of number of malicious programmes and technological refinement of each new malware modification, but also due to the increasing ways in which money and valuable information can be acquired using mobile devices[10].

Kaspersky Lab researchers have seen the number of attacks using malicious mobile software nearly double in just a year. In 2018 there were 116.5 million attacks, compared to 66.4 million in 2017, with a significant increase in unique users being affected[11]. Although an infected mobile software is unlikely to endanger the security of our military system, we have to consider that, on the one hand, we are witnessing a persistent and systematic attack and, on the other hand, the increasing number of attacks should be a wake-up call to start a thorough approach in order to secure our network.

We have shown that every citizen can be the target of a cyber-crime, but this is also an issue for states and private sector. For that purpose, the EU countries have sensed a need to regulate this sensitive issue, materialized in National Cyber Security Strategies.

The cyber security strategy of Romania, aims to define and maintain a secure virtual environment, with a high degree of resilience and confidence, based on national cyber infrastructures, which would constitute an important support for national security and good government, to maximize the benefits for citizens,

[9] See https://www.bitdefender.ro/news/romania-cea-mai-afectata-tara-din-lume-de-amenintarea-informatica-a-momentului-3666.html, retrieved on 26.08.2019.

[10] See https://securelist.com/mobile-malware-evolution-2018/89689/, retrieved on 26.08.2019.

[11] See https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies, retrieved on 26.08.2019.

businesses and the Romanian society as a whole[12]. This very principle is embraced at the European level since the EU's vision in this domain is to clarify the role and the responsibilities and to set out an effective protection and promotion of citizens' rights and to safeguard an online environment providing the highest possible freedom and security for the benefit of everyone[13].

It transpires from the above that at European Union level and in the Member States the action plan priorities are similar. The focus in clearly to maintain a secure environment so that all citizens can enjoy the values of democracy and a safe cyber environment for personal purposes. Moreover, there are concerns on potential security breaches at company level and business environment in general. In this latter case, a security breach will most likely cause significant damage with devastating consequences.

The EU and the Member States need strong and effective legislation to tackle cyber-crime because the evolution of cyber-crime techniques has accelerated rapidly and in this situation law enforcement agencies cannot combat cyber-crime with outdated operational tools. Fortunately, at the European level, we are counting on the continued support of the European institutions to identify gaps and strengthen our capability to investigate and combat cyber-crime.

However, the cyber security concept involves the cyber defence dimension too. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats.

As we have already pointed out, Romania is currently facing threats to its infrastructure originating from cyberspace. This is due to an increasing interdependence between cyber infrastructure and infrastructure such as that belonging to banking, transport, energy and national defence sectors. We see that there is a need for action in these areas in order to meet these challenges.

Most organizations have therefore developed some level of cyber incidence response (CIR) capabilities. Yet those capabilities, which are often weighted toward short-term responses and IT issues, may fail to address all impacts of a cyber incident and keep it from reaching crisis proportions. Avoiding a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds.

In this context, we have to talk about important steps to follow in order to secure our digital data and to have a powerful answer in case of a cyber-attack.

[12] Annex 1 Art. 2, HG. 271/2013 to approve the cyber security strategy of Romania and the national action plan to implement the national cyber security system.

[13] See https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, retrieved on 26.08.2019.

Thereby, experts in this field are talking about risk management in 3 phases with great opportunities to protect the organization from risks, costs and damages and to prepare it for an appropriate response.

Readiness is the phase which involves keeping a well-prepared, multifunctional team that must be able to deal with all aspects of an incident or crisis. During this phase, it is important to provide infrastructure and capabilities for cyber incident exercises, which are essential to stimulate cooperation among state and private sector. Obviously, this course of action involves a large number of cyber security experts. Unfortunately, the expected rise in jobs is outpaced by the expected need for them. By 2021, the number of unfilled cyber security jobs worldwide is expected to break 3.5 million[14]. It is noted that a good cooperation between all competent authorities and private sector depends on our ability to ensure the tuition in this field.

A poor *response*, although it is aimed to eliminate the threats, can create a crisis. Vigorous coordinated response to incidents limit lost time, money and customers as well as damage to reputation of the authority concerned. Management must be prepared to communicate, as needed across all media, including social media, in ways that assure stakeholders that the organization's response is equal to the situation, prompt and effective.

Recovery after a cyber-attack is particularly important. Steps to return to normal operations and limit damage to the organization and its stakeholders continue after an incident. Post-event steps include assessments of the causes and of the management of the incident or crisis and promulgation of lessons learned.

Effective crisis management extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions. The risk that cyber crises pose to reputation and operations emphasize that the time to prepare a highly effective cyber crisis management plan before a cyber incident occurs[15].

So, cyber-crime prevention is the key to keep these phenomena under control. But cyber-crime presents particular crime prevention challenges so that we have to adapt our methods in order to have the expected results. These particularities include the increasing ubiquity and affordability of online devices leading to large numbers of potential victims; the comparative willingness of persons to assume risky online behaviour; the possibility for anonymity and obfuscation techniques on the part of perpetrators; the transnational nature of many cyber-crime acts; and the fast pace of criminal innovation.

[14] See https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/, retrieved on 27.08.2019.
[15] See https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf, retrieved on 27.08.2019.

In this scenario, organizational structures will need to reflect the need for international and regional cooperation in cyber-crime prevention. Methods will need to ensure a constantly updated picture of cyber threats, and approaches will need to involve a range of stakeholders, in particular the private sector organizations that own and operate internet infrastructure and services[16].

The cyber-attacks are various and have a diversity of public and private institutions in their cross-hairs. Those attacks aim all kind of areas from protected health information, payment card data, social security numbers, dates of birth, email addresses or phone numbers to financial or public administration, nuclear facilities or even election process.

Since the 2016 US presidential election and the Russian interference with the electoral process, fears have spread rapidly over the danger of cyber-attacks. However, the European Union acknowledged the importance of cyber security several years prior to the cyber meddling in the US elections.

In 2017, the Commission came up with additional recommendations to enhance cyber-security and encouraged member states to make the necessary investments. Starting from the year 2017, several measures have been taken to strengthen resilience and the ability to respond to major cyber-attacks. Those measures include the establishment of an inter-institutional Computer Emergency Response Team (CERT-EU), which is in charge of a coordinated approach to large-scale cyber-attacks and the development of security certification for products and services across the EU.

Given that we have recently witnessed a very important moment in European politics, the election of the European Parliament, we have to mention that, apart from a direct major cyber-attack, there is a threat of disinformation emanating from foreign power and indirect meddling with the elections. Unfortunately, it is a very frequent and relatively simple way of indirectly influencing voters' public opinions. It is also much easier and safer for a potential attacker to use disinformation than to organize a major cyber-attack. Yet there is little to be done in this regard apart from educating people on media literacy and critical thinking[17].

Going back to our analysis, as we have mentioned, in 2018 the number of cyber-attacks doubled compared with the statistics from 2017 but what is more frightening is that the rate of these crimes is only expected to increase. Criminals are finding increasingly clever and diabolical ways to get their hands on data. In this context, the annual cost of cyber-crime damages is expected to hit $5 trillion by 2020[18].

[16] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime,* New York, 2013, p. 226.
[17] See https://www.esjnews.com/are-european-elections-vulnerable-to-cyber-attacks, retrieved on 27.08.2019.
[18] See https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/, retrieved on 27.08.2019.

Established in Washington, DC, over 50 years ago, the Center for Strategic and International Studies mentioned, in a study updated until August, that more than 60 significant cyber incidents have taken place so far[19]. This study focused on cyber-attacks in government agencies, defence and high- tech companies or economic crimes with losses of more than a million dollars. Now we can have an idea about the magnitude of this security issue.

We must be aware that, in addition to these threats against government and different companies, we are facing a huge risk in terms of digital security for citizens. That is why in EU's and Romania's cyber security strategies are set out a series of measures aimed at promote the security culture in the cyber field. In this regard, we can observe that, in addition to the measures provided for the security of the government, there is a constant necessity to inform the population about the threats, vulnerabilities and risks specific to the use of cyberspace. Moreover, appropriate professional training to people working in cyber security and the widespread promotion of professional certifications field are considered key elements in the consolidation process of citizens' cyber security culture[20].

CYBER SECURITY – A SHARED RESPONSIBILITY

At home, at work and at school, our growing dependence on technology demands greater security online. Individuals are the first line of defence in guarding against online risks. For this reason, cyber security is a shared responsibility, requiring awareness and vigilance from every citizen.

UK Government, in a recent survey, states that over four in ten businesses (43%) and two in ten charities (19%) have experienced cyber security breaches or attacks in the last 12 months. This rises to seven in ten (72%) among large businesses, and a similar proportion (73%) among the largest charities with incomes of £5 million or more. Breaches were more often identified among the organizations that hold personal data, where the staff use personal devices for work or where they use cloud computing[21].

According to a study conducted by Kaspersky half of businesses surveyed believe a lack of knowledge, carelessness or malice on an employee's part could lead to a cyber-attack. Additional research shows 84% of cyber-attack victims attribute the attack, at least in part, to human error. Therefore, they confirm another survey carried out in 2016 by IBM which showed, in 2016 Cyber Security Intelligence Index, that human error is a major factor in breaches, and trusted but unwitting insiders

[19] See https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents, retrieved on 27.08.2019.
[20] Annex 1 Ch. III Art. 3, HG. 271/2013, *cit.doc.*
[21] Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey: Statistical Release, 2018,* p. 1.

are to blame. From misaddressed emails to stolen devices or confidential data sent to insecure home systems, mistakes can be very costly[22].

In response to those challenges, when it comes to prioritization of cyber security actions, we see that the vast majority of the companies see it as a major priority. The risks are understood and therefore the ground for actions is laid out. A percent of 77% of the companies surveyed rank cyber security as a major priority, while 21% consider it a minor priority, and another 2% consider it is not a priority at all[23].

The danger on the Internet exists for absolutely everyone. In cyber security it is often said that zero risk does not exist. People have grown to believe that advancements in technology are the only factor that guarantees their safety, but this view is obviously erroneous. Even though large organizations typically dedicate more attention to security regulations, the breaches often appear inevitable. No matter how much time and money a company invests into security systems implementation, breaches seem to keep occurring. One of the reasons is that nothing, not even in the age of technology boom, can replace people[24].

With an aim of emphasizing the role of people in computer and internet security, we must highlight the need for effective and constant training in cyber security for every employee because sometimes, even the most well-intentioned employee can make mistakes that leave an organization vulnerable to cyber-attacks.

In this framework, ensuring cyber security is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them. Several initiatives have been developed in recent years and should be continued. In particular, ENISA (The European Union Agency for Cybersecurity) has been involved in raising awareness through publishing reports, organizing expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness.

But these measures are not sufficient to reduce the magnitude of the problem here. All these activities undertaken by governments, national and international agencies remain without its intended effect unless the organizations or companies concerned will do their best to educate their staff in order to act according with the cyber security rules.

Considering that in Romania there is a huge lack of experts in this field, it is essential that a critical mass of specialists should be created, sense in which

[22] See https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company, retrieved on 28.08.2019.
[23] See https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf, retrieved on 28.08.2019.
[24] *People's Role in Cyber Security: Academics' Perspective,* 2014, https://www.crucial.com.au/pdf/, retrieved on 28.08.2019.

the government, private sector and the academia must work together to develop learning schemes and training system for computer specialists[25]. Through the same line of action, awareness campaigns must be organized at national level.

The European Information Sharing and Alert System, for example, gathers information and educational materials from computer emergency response teams and other security communities from countries in Europe. Materials have then been adapted for different groups of citizens and small and medium size businesses in each participating country. Materials have been disseminated using social media, websites and mailing lists. A large-scale pilot programme focused on awareness of botnets, identity theft and social engineering threats reached over 1,500 people.

Technology companies and non-profit groups have also run their own awareness-raising campaigns. Google's *Good to Know campaign*, for example has run in around 40 languages since

2011. Adverts in newspapers, magazines, online and on public transport give security tips and explain some basic internet features such as cookies[26] and IP addresses[27]. The Family Online Safety Institute has also worked with technology companies to aggregate educational resources for parents, children and teachers at their *Platform for Good website*. For a younger audience, Disney ran a TV, website and magazine safety campaign in 2012 aimed at 100 million children and parents in Europe, the Middle East and Africa[28].

So, if at the level of some huge companies there are sizable sufficiently concrete measures, at the level of an institution, what steps can be taken to pursue a safer cyber space, which are the most common employee mistakes and what can we do to fix them?

First step is to invest more time and money into training employees on the data dangers they all face. Only when employees are educated can be taken steps to avoid little mistakes that turn into big cyber issues. They often think of their credit card information on apps and websites, but what often does not come to mind is email security. In the past years there have been multitudes of data compromised all due to the theft of consumers[29], otherwise known as your online identity. This will continue to be one of the biggest risks for businesses and consumers in the years to come too.

Besides social media, email is one of the top ways we communicate online.

[25] Romanian Intelligence Service, *Buletin Cyberint*, semester 1-2019, p. 11.

[26] A small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. Cookies were designed to be a reliable mechanism for websites to remember stateful information.

[27] An IP address serves two main functions: host or network interface identification and location addressing.

[28] United Nations Office on Drugs and Crime, *Comprehensive study on Cybercrime,* New York, 2013, p. 227.

[29] Personally identifiable information, or PII, is any data that could potentially be used to identify a particular person.

A consumer's email address is the online ID. Think of the information people send over via email: address, bank information, health information and documents, legal information etc. Tracking and postmarking electronic communication is a great way to secure your emails to make sure they are going where they should, and to whom they should[30]. The employees should not open emails, attachments or links from people they do not know.

Repetitive passwords that use personal information, such as a nickname or street address, are a problem. The problem is that 81% of adults use the same password for everything. Therefore, it is necessary to create rules that require employees to create unique, complex passwords and to change them if they ever have reason to believe that they have been compromised.

Research shows the majority of companies do offer cyber security training. It is a great example to follow for public sector in order to provide annual cyber security awareness training to every employee because people will always be behind every automated task and on the other end of every phone call, email and chat session[31]. The only defence against an attack is education or, in industry terms, the security awareness training.

Security Awareness Training generally consists of repetitive training and ongoing, sometimes random, testing. Also, this type of training includes discussion about password management, how to manage mobile devices, relevant examples of situations, safe surfing on web or spam email.

After this type of training, the organization should measure its effectiveness through objective criteria and assess whether the learning process inspired users to apply what they learned. Have they transferred the lessons learned to their jobs? Has training produced results?[32]

The cyber security culture needs to place greater emphasis on **integrating security from an early stage in every structure and to be perceived as an extremely important matter, as a concept that belongs to everyone.**

CONCLUSIONS

Cyber security is now one of the greatest business but it can also be a very sensitive area and one that has the potential to do the most damage to an organization. Dealing with it must be in line with technological development in order to find the best way to maintain a secure the cyber space.

[30] See https://digitalguardian.com/blog/cybersecurity-risks-2019, retrieved on 29.08.2019.

[31] See https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability, retrieved on 29.08.2019.

[32] Society for Human Resource Management, *Implementing effective cyber security training for end users of computer networks,* Virginia, 2015, p. 13

Solutions to cyber security training challenges require an interdisciplinary approach and a permanent cooperation between public and private sectors. Health and safety at work is now the norm and is rarely considered anything other than standard. Cyber security has to reach the same level of acceptance, involvement and implementation by in-depth insights into the human factor.

Cyber security is a global problem, and we are all in this together. We cannot expect that a lone attacker sitting in a country and conducting multiple cyber-attacks is an isolated threat. In this case, everybody should cooperate and communicate in order to create a common response, flexible enough to work perfect in every situation.

We must always remember that security belongs to everyone, from the executive staff to the lobby ambassadors. Everyone owns a piece of the company's security solution and security culture because security systems cannot guarantee protection as long as people neglect their parts of this immensely important responsibility.

Cyber security is a never-ending battle. A permanently decisive solution to the problem will probably not be found, or, at least, not in the near future. Given these circumstances, we need to focus on concrete measures and launch sustainable solutions and procedures in this sensitive sphere.

BIBLIOGRAPHY

1. ***, Department for Digital, Culture, Media&Sport, *Cyber Security Breaches Survey: Statistical Release*, 2018.
2. ***, Hotărârea Guvernului no. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică.
3. ***, *People's Role in Cyber Security: Academics' Perspective*, 2014.
4. ***, Romanian Intelligence Service, *Buletin Cyberint semestrul I*, 2019.
5. ***, Society for Human Resource Management, Implementing Effective Cyber Security Training for End Users of Computer Networks, Virginia, 2015.
6. ***, United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, New York, 2013.
7. Jochen Rehrl, *Handbook for Decision Makers – The Common Security and Defence Policy of the European Union,* Imprimerie Centrale, Luxembourg, 2017.

WEBOGRAPHY

1. https://www.bitdefender.ro/news/romania-cea-mai-afectata-tara-din-lume-de-amenintarea-informatica-a-momentului-3666.html
2. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
3. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

4. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf
5. https://digitalguardian.com/blog/cybersecurity-risks-2019
6. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
7. https://www.enisa.europa.eu/topics/incident-reporting?tab=details
8. https://www.enisa.europa.eu/media/multimedia/videos/cybersecurity-is-a-shared-responsibi lity-european-cyber-security-month-2018
9. https://www.esjnews.com/are-european-elections-vulnerable-to-cyber-attacks
10. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company
11. https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies
12. https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf
13. https://www.nato.int/cps/en/natolive/official_texts_17120.htm
14. https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability
15. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
16. https://securelist.com/mobile-malware-evolution-2018/89689/

THE BLACK SEA MILITARISATION

Marius ȘERBESZKI, PhD
Senior Lecturer, "Carol I" National Defence University, Bucharest

Romania, by the nature of its political orientation, its Euro-Atlantic community membership, the specific agreements, treaties and undertaken partnerships, as well as its geographical position, lies at the Eastern border of both EU and NATO. As a result, one of the assigned missions of its air and naval forces is the monitoring of the situation developments in the Black Sea region, in order to ensure the early warning and useful information needed at strategic and operational decision-making levels.

The occupation of the Crimean Peninsula, its saturation with troops and military equipment by the Russian Federation and the public declarations of Russian officials, referring to some NATO countries, have generated a lot of tension and uncertainty in the region. All the mentioned aspects have led to the Black Sea area gradual transformation, from a quiet area of free trade and the germ of economic development at regional level, to a "stormy" area between the Russian Federation and the West.

The connection between action and reaction causes a cyclical effect, as in any system. In that manner, the consolidation of Anti-Access Area Denial (A2AD) capabilities by a state will generate, even though only as a precaution, a sustained effort from another state or coalition of states to find out a solution to counter them.

Keywords: Black Sea militarisation, Anti-Access Area Denial, Crimean Peninsula, Ukraine, Russia, Romania.

WHY IS THE BLACK SEA SO IMPORTANT?

The Black Sea region forms a key intersection, linking mainland Europe, Russia, the Caucasus, the Middle East and Central Asia. For more than two centuries, Russia endeavoured to establish exclusive control of the Black Sea and waged numerous wars against Turkey in order to capture the Bosporus Strait and lock the Black Sea for its own use. During the Cold War, the Black Sea was virtually a Soviet lake. Nowadays, the Black Sea remains a strategic crossroad for the entire region.

The Black Sea region has also an enormous economic potential, being a transit area for goods, with a continental shelf that possesses abundant natural resources, including natural gas deposits, as well as an area for fishing and tourism. Moreover, it is an important energy route and an area rich in cultural and ethnic diversity, where several conflicts are more or less frozen.

Nonetheless, the access to the sea is of vital importance for all littoral and neighbouring states as it greatly enhances the projection of power into several adjacent regions.

WHAT IS A2AD?

The US *"Joint Concept for Access and Manoeuvre in the Global Commons"* (subsequently renamed *"AirSea Battle Concept"*[1]) defines *"Anti-Access"* in relation to the actions and capabilities – usually long-range ones – designed to prevent forces from entering a region, while *"Area Denial"* – usually short-range – aims at limiting an opponent's freedom of action and manoeuvre in the operational area.

Sam Tangredi, in his book *"Anti-Access Warfare. Countering A2AD Strategies"*, states that *"the combination of anti-access and area denial refers to warfighting strategies focused on preventing an opponent from operating military forces near, into, or within a contested region"*[2]. The key task of any defender is to prevent an opponent to operate its military forces close to its centre of gravity. Therefore, *"the objective of an anti-access or area denial strategy is to prevent the attacker from bringing its operationally superior forces into the contested region*

[1] ***, *Air-Sea Battle*, Service Collaboration to Address Anti-Access & Area Denial Challenges, Air-Sea Battle Office, May 2013.
[2] Sam Tangredi, *Anti-Access Warfare: Countering Anti-Access and Area-Denial Strategies*, Naval Institute Press, 2013, p.14.

or to prevent the attacker from freely operating within the region and maximising its combat power"[3].

A2AD is by no means a new concept. However, it is based not only on historical precedents, such as the Ottoman defence of Straits (1915-1916) and the Battle of Britain (1940), but also on new technologies that have changed the scale, lethality and scope of the threat. Although this concept was used throughout history mostly by the Land Forces of the states that had little or no naval power, nowadays, the Air Force and the Navy identify themselves with this concept, due to their inner capability to operate over long distances, to connect their weapons and command and control systems, in order to create overlapping layers to protect a space, an area or a territory.

WHAT IS RUSSIA DOING IN THE BLACK SEA?

The main objective of Moscow's politics in the Black Sea area is to assume a dominant position, which was lost because of the collapse of the Soviet Union, the NATO and EU membership of Romania and Bulgaria and the refusal of Ukraine and Georgia to remain in Russia's sphere of influence. The Black Sea is of vital importance to Russia from a strategic point of view, this area being not only a space for affirming its regional interests, but also one for expressing the global ambitions of President Putin.

To carry out A2AD tasks an entire range of assets are employed, including ballistic missiles (BMs), surface-to-air missiles (SAM), anti-ship missiles (ASM), cruise missiles, bombers, fighter jets, submarines, mines, drones and EW means. Such measures are asymmetric, and are often used by potentially weaker countries, which derive advantages from the operation in the vicinity of their territory.

Since its attack on Ukraine, Moscow has enhanced its status as a maritime power in several ways. The integration of Crimea provides Russia with an additional coastline of several hundred kilometres, together with the crucial Black Sea port of Sevastopol. Its Black Sea fleet is positioned to deny military access to the Caucasus and to Ukraine. It has been incorporated into Russia's southern military district and now fulfils several roles, including securing navigation and sea lines of communication, countering the presence of naval groups of NATO forces, supporting units coming from other Russian fleets operating in the Mediterranean and maintaining leverage over energy supplies from the Caspian Basin to Europe. The expansion and modernisation of the Black Sea fleet have become some of the Kremlin's highest priorities. By 2020, Russia plans to significantly enhance its military presence in Crimea, while deploying additional mobile missile coastal

[3] *Ibidem*, p. 15.

forces, surface-to-air missile systems, long range bombers, new class submarines, enhanced radars and even nuclear capabilities.

Within the Black Sea, Crimea became Russia's main platform for conducting A2AD operations. Advanced defence systems have been deployed to the peninsula, such as the anti-ship Bastion-P missile system equipped with the P-800 Oniks cruise missiles, along with the surface-to-air S-300 and S-400 Triumf missile systems. Upgrade programmes are underway to refurbish Soviet-era bunkers, reanimate early warning radar systems, and install high-tech electronic warfare equipment. Along with Russia's other missile systems in Armenia, Krasnodar, and Latakia, its A2AD capabilities extend over major parts of the region, covering much of the Black Sea, and parts of Moldova, Romania, Georgia, Turkey, and Ukraine.

Figure 1 – Russia improves military infrastructure in the Crimean Peninsula[4]

The Black Sea Fleet is also undergoing a major modernisation programme. Moscow plans to spend $2.4 billion by 2020 to provide the fleet with next-generation warships, submarines, and air defence systems. Up to eighteen new units have been commissioned and many will be equipped with the versatile Kalibr-NK missile system. They will be joined by new air assets such as the Su-30M naval aviation fighter and other air-to-ground attack fighters and helicopters.

[4] Source: *Russian Military Aggression against Ukraine. Presence of the Russian Armed Forces on the Occupied Territories of Ukraine – Autonomous Republic of Crimea and City of Sevastopol - May 2016*, see www.slideshare.net/EmbassyUkraine/ppt0000003-61701174, retrieved on 16.05.2019.

All these capabilities are meant to transform the Black Sea Fleet into a force capable of denying NATO access to the Black Sea and projecting power to threaten NATO interests in the Mediterranean and the Middle East.

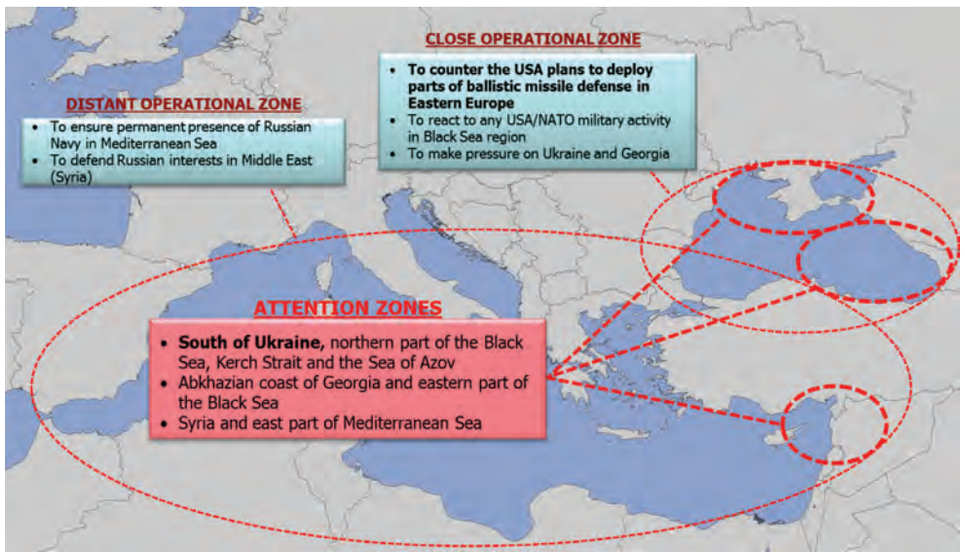


Figure 2 – Russia's area of interest in the Black Sea and the Mediterranean Sea[5]

Russia's A2AD capabilities will also be strengthened by the deployment of the Tupolev Tu-22M3 nuclear-capable strategic bomber to the region. The long-range bomber can carry Kh-15 or Kh-22 missiles designed to destroy air defence systems. The bomber force will be protected by Russian fighters like the Sukhoi Su-24 which can secure a vast part of the Black Sea airspace and greatly expand Russia's strategic aviation patrol routes in the region.

… AND WHY?

In deploying these capabilities together with the missile systems, Russia would be able to form a multi-layered, interconnected defence network that can threaten or interdict any force within the A2AD bubble.

The Kremlin is increasingly able to deploy long-range, anti-ship and anti-aircraft missiles to strike ground targets, interdict maritime traffic on the Black Sea and impose no-fly zones around the Black Sea littoral. Airborne troops, naval infantry and Spetsnaz (Special Operations) forces could also be stationed in Crimea

[5] *Source: Russian Military Aggression against Ukraine. Presence of the Russian Armed Forces on the Occupied Territories of Ukraine – Autonomous Republic of Crimea and City of Sevastopol - May 2016*, see *www.slideshare.net/EmbassyUkraine/ppt0000003-61701174,* retrieved on 16.05.2019.

Figure 3 – Russia's A2AD capabilities in the Black Sea area[6]

for potential deployment elsewhere. In early March 2015, President Putin suggested that Moscow could deploy nuclear weapons in Crimea. The Iskander tactical ballistic missile (either in conventional or nuclear form) has a 400-kilometre range and could reach the entire southern part of Ukraine, including the important industrial cities of Odessa, Krivyi Rih and Dnipropetrovsk, a large part of Moldova, the entire Romanian coastline and a significant portion of the Turkish Black Sea coast. In fact, it can be stated that Moscow is developing capabilities to *"sequester"* the Black Sea and to deter adversaries from entering this area to counter Russia's offensive.

By dominating the Black Sea, Russia has the capacity to project its military power toward the eastern Mediterranean, the northern Middle East, the South Caucasus, and toward the rest of mainland Europe. Control over regional ports and sea lines of communication would enable Russia to *"choke"* the trade routes and disrupt the energy supplies via pipeline from the Caspian Basin to Europe, to prevent NATO from projecting sufficient security for its Black Sea members (Romania, Bulgaria and Turkey), and to deter the intervention of littoral states on behalf of vulnerable neighbours.

[6] *Source: Russian Military Aggression against Ukraine. Presence of the Russian Armed Forces on the Occupied Territories of Ukraine – Autonomous Republic of Crimea and City of Sevastopol - May 2016*, see *www.slideshare.net/EmbassyUkraine/ppt0000003-61701174,* retrieved on 16.05.2019.

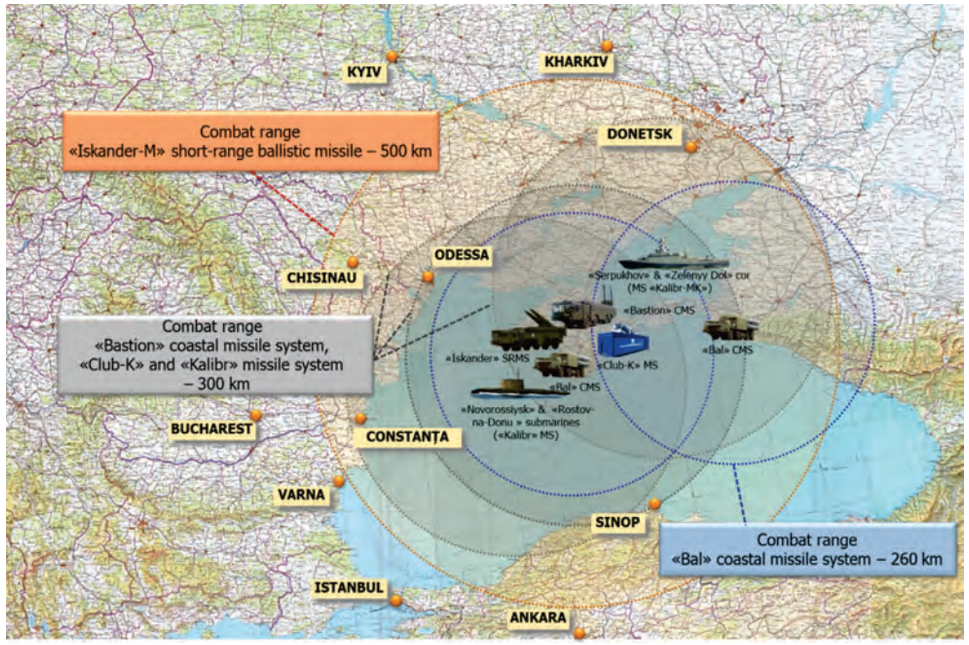


Figure 4 – The combat ranges of several Russian capabilities deployed in the Black Sea area[7]

A ring of smouldering conflicts surrounds the Black Sea. In Moldova, a 28-year-old frozen conflict divides the country into two pieces. Ukraine's Crimean Peninsula was already annexed by Russia, and the Donbass region remains occupied by Russian-backed separatist forces. Russia's main supply route to its forces in Syria runs through the Black Sea via the Bosporus and Dardanelles to the Eastern Mediterranean. In the Caucasus, ongoing conflicts between Armenia and Azerbaijan over Nagorno-Karabakh region and between Georgia and the breakaway regions of South Ossetia and Abkhazia continue to attract the interest of outside powers, Russia being chief among them. Historical grievances and ethnic tensions could be harnessed by Moscow as a means to interfere in its neighbours' affairs and pressure regional governments into aligning themselves with Russia. By *"turning"* regional NATO members, Moscow could severely weaken the Alliance's internal cohesion and undermine its credibility.

Moscow's propaganda and disinformation campaigns aim to discredit pro-Western and liberal governments throughout the region, while favouring parties and factions more amenable to Russia's influence. The Kremlin seeks to build special relations with individual countries in order to weaken regional solidarity and joint

[7] *Source: Russian Military Aggression against Ukraine. Presence of the Russian Armed Forces on the Occupied Territories of Ukraine – Autonomous Republic of Crimea and City of Sevastopol - May 2016*, see *www.slideshare.net/EmbassyUkraine/ppt0000003-61701174,* retrieved on 16.05.2019.

action. In some cases, Moscow can trigger or create new protracted conflicts in territorial enclaves and border regions.

With regard to Romania, the Kremlin may endeavour to manipulate the latent *"Greater Romania"* idea to promote regional disputes with Moldova and Ukraine, infiltrate saboteurs, orchestrate protests and support separatist activities like those of Hungarian-Székelys (Szeklers) in Transylvania. There is also a risk of disruption to Romania's exploration of Black Sea natural resources through either harassment or a legal dispute involving territorial waters claimed by Russia, since it annexed Crimea. Moreover, tourism and commercial trade through the ports of Constanța or along the Danube River can be unsettled.

An expansion of Russia's proxy war in eastern Ukraine toward Odessa and the Ukrainian side of the Danube Delta could also choke this critical artery and create important losses for the countries using the Danube as a trade access point to the heart of Europe.

WHAT SHOULD WE (NATO) DO?

Since the Russian annexation of Crimea, NATO has been strengthening its deterrence potential. However, it still respects the 1997 declaration on refraining from permanent deployment of substantial combat military forces on the territory of its new members. After the 2014 NATO Summit in Newport, the Alliance has improved its ability to deploy a rapid response force (NRF) on the Eastern Flank, including to Bulgaria and Romania. However, before the July 2016 Summit in Warsaw, Romania (like Poland and the Baltic States), sought to create a deterrence mechanism based on a continuous, rotational NATO presence. Because of Romania's geographical position and the threat of a Russian amphibious assault, Bucharest called for the establishment of a NATO naval mission in the Black Sea. Just before the summit, Bulgarian Prime Minister Boyko Borisov said that his country did not feel threatened by Russia, and that the deployment of permanent naval forces could be provocative. Turkey did not back the Romanian proposal either, as Ankara has been seeking to improve relations with Russia since the downing of a Russian aircraft in November 2015. Turkey also feared that it would bear the main burden of a NATO presence, as the Montreux Convention limits access to the Black Sea by warships from non-littoral states.

Turkey, Romania and Bulgaria finally reached a compromise position, which was approved by NATO defence ministers during the North Atlantic Council (NAC) meeting. The presence of NATO ships in the Black Sea will be enhanced, and they will be put under the command of the Alliance's Standing Naval Forces (respectively, the Standing NATO Maritime Group 2 – SNMG 2) operating in the Mediterranean. In this way, the Supreme Commander of Allied Forces in Europe (SACEUR) will have

the operational command, and will be better able to monitor threats from Russia and react faster to any indications of crisis.

The NATO presence in the region consists of two additional elements. During the NATO Warsaw Summit, the Allies agreed to enhance the air force presence in Bulgaria and Romania, which will help monitor airspace and facilitate a joint threat assessment.

The US troops, present in the region in the framework of the Black Sea Rotational Forces initiative, are the main pillar of deterrence in the Black Sea. The US Navy's Arleigh Burke-class guided-missile destroyers, armed with Aegis air defence systems have been regularly entering the Black Sea. All the mentioned aspects indicate that the US is able to deploy the forces necessary to neutralise the threat posed by Russian offensive capabilities in the region, including Moscow's rhetoric on using nuclear weapons. The rotational presence of the US troops also increases the credibility of the USA commitment to defend Allies in the event of a conflict.

From a purely military perspective, NATO should consolidate its capabilities in order to:

- deploy into a South-Eastern theatre of operation to a position where the Joint Task Force can be employed effectively and with acceptable levels of risk;
- effectively command and control the Joint Task Force in a heavily disrupted electromagnetic-spectrum environment;
- deter an adversary through demonstration of capability, presence and will;
- conduct operational manoeuvre (movement in combination with fires) in an operational area with acceptable levels of risk;
- project power as needed to achieve objectives;
- sustain and supply operations in the face of determined opposition.

CONCLUSIONS

The Black Sea forms a zone of vulnerability for the eastern flank of the Alliance. NATO cannot allow an ambitious adversary to threaten any of its littoral member states (Romania, Bulgaria and Turkey), or the Alliance may lose its credibility as a security organisation. The West has also a keen economic interest in diversifying energy sources and upholding routes from the Caspian Basin, in which the Black Sea forms a network for energy deliveries and pipelines to Europe outside of Russia's control.

From energy to economics, from security to geopolitics to military, the region's relevance is far broader than most people realise. I dare to say that the future of Europe and Eurasia is being contested in the Black Sea.

The annexation of the Crimean Peninsula has allowed Russia to transform the Azov Sea into an internal lake and to impede the normal functioning of the Berdiansk

and Mariupol harbours. Moreover, the Kerch Strait incident in November 2018 is of the same nature. Russia already proved the capability to *"close"* vast areas of the Black Sea in July 2019, under the pretext of military exercises (a total surface of 118.570 sq. km.), blocking the international maritime routes to Bulgaria, Georgia, Ukraine and Romania. *"Together with the militarisation of Crimea, the amplitude of the military exercises in the Black Sea area continues to increase. In this respect, are rehearsed several scenarios of a military conflict between Russia and NATO on Ukraine's territory, the Russian army practicing both offensive and defensive tasks. Besides these conventional military exercises, Russia uses an arsenal of hybrid tools in order to attain its objectives. The large-scale operations in this type of new generation warfare include all the possible measures to attain strategic objectives as disinformation operations, economic pressures and energy supplies pressures, cyber-attacks or psychological operations, in order to create chaos and to lead to the disintegration of the state. The lessons learned in 2008, in Georgia, show the improvement of the employment of the hybrid tools by the Kremlin which will be subsequently used against Ukraine: the exploit of the weak points, of the internal crisis, in order to re-establish the buffer zone between Russia and NATO"*[8]. Therefore, NATO's inaction would greatly enhance Russia's prestige, demonstrating its ability to challenge the West. This should not happen!

BIBLIOGRAPHY

1. ***, *Air-Sea Battle*, Service Collaboration to Address Anti-Access & Area Denial Challenges, Air-Sea Battle Office, May 2013.
2. ***, Defense Express, *Militarisation of Occupied Crimea – a Threat to Global Security*, https://defence-ua.com/index.php/en/publications/defense-express-publications/914-militarization-of-occupied-crimea-a-threat-to-global-security.
3. ***, *Russian Military Aggression against Ukraine. Presence of the Russian Armed Forces on the Occupied Territories of Ukraine – Autonomous Republic of Crimea and City of Sevastopol - May 2016*, *www.slideshare.net/EmbassyUkraine/ppt0000003-61701174.*
4. ***, *Russia Hastily Revamps Soviet Missile and Radar Bases in Crimea*, https://defence.pk/pdf/threads/russia-hastily-revamps-soviet-missile-and-radar-bases-in-crimea.459144/.
5. ***, New Strategy Centre, Summary of the *Security Challenges in the Black Sea Area. Current Situation and Possible Evolutions* event, 11 September 2019, Bucharest, Romania.
6. Nicholas Larrinaga, Sean O'Connor, Neil Gibson, *Russia Reveals Bastion-P Deployment, Land Attack Role in Syria*, IHS Jane's Defence Weekly, http://www.janes.com/article/65517/russia-reveals-bastion-p-deployment-land-attack-role-in-syria
7. Sam Tangredi, *Anti-Access Warfare. Countering Anti-Access and Area-Denial Strategies*, Naval Institute Press, USA, 2013.

[8] The summary of the *"Security Challenges in the Black Sea Area. Current Situation and Possible Evolutions"* event held on 11 September 2019 in Bucharest, Romania.

EXTENDED BLACK SEA REGION – AN AREA OF GEOPOLITICAL CHANGES –

Vasile CERBU, PhD
2nd Infantry Division "Getica"

Valentin CIORANU
582th Reconnaissance Regiment "Vlad Țepeș"

The Black Sea is a security complex that has come to the fore today as a result of the geopolitical changes in recent years. The changes have the effect of modifying the borders. Moreover, new "frozen conflicts" have emerged. The area has gained consistency in the increased attention paid by Turkey and the Russian Federation but also by the US and NATO being positioned on the border of Europe with Asia and with the new great Middle East. It is the source of risks with still imprecise effects defined, having a very high destabilizing potential with implications that can even be global.

In the past years and in the context of the changes in the policy of all the actors in the area, in the paradigm of NATO Defence, a new type of conflict, the hybrid conflict has emerged, and/or specific measures to counteract its effects have been generated. Also, a new arms race began with the involvement of all actors with influence and interests in the region including Romania. We can say that Romania is in the middle of a "perfect storm".

Keywords: geopolitical changes, hybrid war, frozen conflicts, economic opportunities, arms race.

INTRODUCTION

From the earliest times, the Black Sea Region (BSR) has been the meeting point for some advanced civilizations, for expansionist ambitions of some great empires, for military and economic confrontations for the domination and control of this area. First were the Greek cities which, starting with the 7th century BC, established commercial colonies along the shores[1]. Then, starting in the 3rd century AD, the Byzantine Empire, for over a millennium, dominated this space through selective military interventions but also through a complicated system of alliances.

Starting in the 7th century, the Tartars appeared and managed to control a segment of the Silk Road, which linked China and Europe, Geneva and Venice, which founded and developed in the BSR flourishing trade centres that managed to withstand until the 15th century when they were conquered by the Turks. In the 15-18 centuries the area was dominated by the Ottoman Empire which, starting in the second half of the 18th century, was confronted with the expansionist tendencies of the Tsarist Empire, eager to secure exits to the warm seas, which assumed the role of leader of the liberation struggle to the Christian peoples of the Balkans and the Caucasus aiming to conquer the Bosporus and Dardanelles straits[2].

Key moments in the region's history were represented by the Crimean War of 1856-1859 and the First World War of 1916-1918. The Crimean War, which resulted in the weakening of the power and influence of the Ottoman Empire, ended with the defeat of the Tsarist Empire and paved the way for the independence of the states (under Ottoman rule), west of the Black Sea and of the entire Balkan Peninsula. Following the First World War, the dissolution of the Ottoman and Tsarist empires had the effect of reconfiguring the ratio of forces in the region and polarizing the political actors in supporters or opponents of the territorial status quo achieved by the Paris Peace Treaty.

Disputes between the great powers were also regarding the regime of Bosporus and Dardanelles, which was regulated by the Montreux Convention of 1936, still in force today, even if it reflects the political and technical conditions specific to the time in terms of tonnage and the duration of the stationing of military vessels in the area of the non-costal states[3].

[1] *De ce contează Marea Neagră,* Policy Paper New Strategy and Center for American Sea Power (Hudson Institute, USA) Romanian language version, see https://newstrategycenter.ro/wp-content/uploads/2016/049...iunie_2016_1.pdf, retrieved on 18 September 2019.
[2] *Ibidem*.
[3] Dominic Lieven, *Dilemmas of Empire 1850-1918, Power, Territory, Identity*, Journal of Contemporary History, vol. 34 no. 2, April 1999, p.172.

CHARACTERIZATION OF THE EXTENDED BLACK SEA REGION

The acceleration of the process of globalization as well as the political, military and economic mutations that have occurred worldwide, but especially in the European space, have provided the Black Sea region with a special economic and geostrategic importance, not only for the states of the area but also for NATO, the EU or other global or having global ambitions actors. The Black Sea region is part of a process that has not ended, of eliminating the legacy of the Cold War[4], but also of one that started and is in the process of reconfiguration of the geo-political system, to reaffirm the role of the Russian Federation as a global player and to readjust the role of Turkey, both within NATO and within other security arrangements that include south-eastern Europe but also Central Asia and the Middle East

The area became a security complex in the late 1990s as a result of the evolution of post-Cold War relations. The Black Sea region, as a security complex, is located between three security macro-complexes, consisting of the Euro-Atlantic bloc, the New Middle East and the former Soviet space[5]. These macro-complexes are separated by faults that interconnect and form a strategic imaginary triangle that overlaps the Black Sea.

In recent years, the Black Sea region has gained consistency, embodied in the attention given by the EU, NATO, but also the USA as a global player. Attention is generated by factors of a geopolitical, military and economic nature.

It has come to the attention of the whole world that by reactivating its destabilizing potential, especially through the Georgian War (2008), the annexation of Crimea (2014) and the events in eastern Ukraine started in 2014 and still unresolved[6].

There is no unanimously accepted definition of the Black Sea region, neither in the political environment nor in the scientific one. In the acceptance of the institutions of the European Union, the Black Sea Region represents a distinct area that brings together ten states, six neighbouring states (Romania, Russian Federation, Georgia, Turkey, Ukraine, Bulgaria) and four non-costal states (Azerbaijan Armenia, the Republic of Moldova and Greece), whose history, neighbourhood and close relations with the Black Sea region recommend them as actors with a certain relevance[7]. The term extended is, we can say, of recent time and its use is in particular related to the geopolitical and geostrategic design of the manifested interests, regarding

[4] Adrian Pop, Dan Manoleli, *Toward a European Strategy in the Black Sea Area: The Territorial Cooperation*, Strategy and Policy Studies. No 2007, 4, European Institute of Romania, Bucharest, December 2007, p. 9, see ier.gov.ro/wp-content/uploads/publicatii/spos_2009_4_en.pdf, retrieved on 07 September 2019.

[5] See http://www.facebook.com/notes/iulian/chifu-istoria-unui-concept-de-seciritate-in-regiunea-extinsa-a-Marii-Negre/, retrieved on 06 September 2019.

[6] Petrică-Lucian Foca, Vasile Cerbu, *Romania the Country in the Middle of a "Perfect Storm"*, *Romanian Military Thinking*, no. 4/ 2016, p. 36.

[7] Andrei Pop, Dan Manoleli, *quoted opus*, pp. 9-10.

this space. Therefore, we can say that the Extended Black Sea Region includes the area between the Balkan Mountains and the Caspian Sea, and has become one of the most dynamic areas during the post-Cold War and post-Soviet period[8].

Figure no. 1- Extended Black Sea Region[9]

The Extended Black Sea Region is a security complex that, according to Buzan and Waever, (security theorists, representatives of the Copenhagen school), groups the states in the region and their security is easily distinguished from the neighbouring security regions[10].

The Black Sea Security complex groups states whose major security perceptions and concerns are interconnected at a very high level, so that their international security issues can only be fully analysed and resolved[11]. The Extended Black Sea Region is a security complex where the dominant factor is confrontation, without missing the specific actions of cooperation. The most important confrontations are between Russia and Georgia (2008), between Russia and Ukraine since 2014,

[8] Florin Iftode, *Amenințări și vulnerabilități la adresa securității în zona extinsă a Mării Negre*, see ibn.idsi/sites/default/fies.imag_file/Amenintari_si_Vulnerabilitati_a_adresa_securitatii/o_pdf, retrieved on 10 September 2019.

[9] See https://titulescu.eu/2011/05zona-extinsa-a-marii-negre-povara-sau-sansa-pentru-riverani, retrieved on10 September 2019.

[10] Cristina Bogzeanu, *Evoluția mediului de securitate în zona extinsă a Mării Negre și influența acesteia asupra configurării forțelor navale ale României pe termen mediu și lung*, Editura Universității Naționale de Apărare, "*Carol I*", București, 2012.

[11] Barry Buzan, Ole Waever, *Security a New Framework for Analysis*, CA Publishing, Cluj-Napoca, 2011, pp. 27-28.

between Azerbaijan and Armenia. In this pattern of confrontation can be framed the dispute between Romania and Ukraine regarding the delineation of the continental shelf of the Black Sea, supported by the arbitration of the International Court of Justice in The Hague.

The importance of the Extended Black Sea Region is highlighted by several main aspects as follows:

- it represents the interference space of three geopolitical and geostrategic areas facing particular security and stability problems: southern Europe, Eastern Europe, and the Middle East;
- it is crossed by two major geopolitical axes: the north-south axis which includes Russia, Armenia and Iran and the east-west axis, which includes Central Asia, the Caucasus, and the Balkans;
- it represents the gate to the warm seas and the planetary ocean for Russia, Romania, Bulgaria, Ukraine, Trans-Caucasian countries, including for the countries of Central Asia bordering the Caspian Sea (through the Volga-Don canal[12]);
- it represents an important segment of the southern border of Russia;
- it is the border of the south-east flank of NATO;
- it is a vital point for a series of strategic flows: the flow between energy producers (Russia and the countries of the Caspian and Middle East areas) and energy consumers (Euro-Atlantic area); security flow between the Euro-Atlantic community – security provider and security consumers (Middle East and Central Asia[13]);
- three of the four strategic European routes (European, Danube and Southern maritime) influence the eastern part of the Black Sea including Romania;
- it is the contact area of two religions: Christianity and Islam;
- it is the contact area between the European Union and the North Atlantic Alliance (adept of the thalassocracy ideology) and the Russian Federation (adept of the telurocracy ideology); the states of these two blocs are thus, the followers of two antagonistic ideologies, bringing in policies based on the strength of the water areas, respectively of the dry areas[14];

[12] Volga-Don Canal ensures navigation between the Caspian Sea and the Black Sea. It was built during Peter the Great time between 1701-1707. In the current form, this project was completed in 1952, requiring a huge effort of 900,000 workers and 100,000 German prisoners and 100,000 detained in the gulag. The canal has 9 locks and a single room on the slope from Volga that can lift the vessels to 88 meters and 4 locks of the same kind on the slope from the Don which can lower the ships by 44 meters and can serve ships of 5000 tdw, 140 meters long, 16.6 meters wide and 3.5 meters draft.

[13] Gheorghe Văduva, *Falia strategică Marea Neagră-Marea Baltică*, see http://revistapolice.ro/falia strategica-marea -neagra-marea-baltica/ retrieved on 07 September 2019.

[14] Aydin Mustafa, *Regional Cooperation in the Black Sea and the Role of Institutions*, in Perceptions, Autumn, 2005, pp. 5-60.

- it is the area where conflicts have generally arisen on ethnic criteria, which are in the stage of frozen conflicts with weak hopes of being resolved soon (Transnistria - Republic of Moldova, South Ossetia and Abkhazia in Georgia, Nagorno-Karabakh-Armenia and Azerbaijan, Donetsk and Lugansk-Eastern Ukraine)
- it has the energy dimension represented by the control of the transport routes of the crude oil and natural gases, the extraction of these existing deposits within this area[15].

As Central Asia and the Caucasus represent the strategic energy corridor of the Eurasia, the vast Black Sea region has played and continues to play a key role in shaping the Eurasian space in the European and Euro-Atlantic vision. The Black Sea represents a binder in this space, besides the three European strategic corridors already mentioned, there are several strategic corridors open to the Asian space such as: the Caucasian energy corridor, the Caspian Sea, Central Asia, the Strategic South-East Asian corridor, the western Black Sea, Turkey, Mesopotamian plain, Persian Gulf and Strategic Don corridor, Western Siberia Volga.

Figure no. 2: Main gas pipelines routes from the Extended Black Sea Region[16]

[15] Marius Roșu, Summary of the PhD thesis with the theme *Political Considerations over Extended Black Sea Region*, see https//www.unap.ro/ro/doctorat/teze_doctorat/2016_ianuarie ROSU-MARIUS. Pdf, retrieved on 17 September 2019.

[16] Maps: iran-resist.org/article 2357, retrieved on 02 September 2019.

RISKS AND THREATS IN THE EXTENDED BLACK SEA REGION

The Extended Black Sea Region, as mentioned above, is a space through which contact with other regions is made, being exposed to risks and threats.

The security environment in this region is in a continuous transformation and it is characterized by complexity and dynamism as a result of the strategic and military repositioning of the states with interests in the area but also as a result of the political, economic and technological conditions generated by the phenomena specific to globalization. At the same time, the situation in the region will be characterized by predictable and linear manifestations, which represent effects of strategies applied by some state and non-state actors in the long term, but also manifestations having a deep, unpredictable, nonlinear and disturbing character, which can generate surprises[17].

Figure no. 3: Main instability centres in EBSR[18]

The main threats, risks and vulnerabilities are of social economic, political, technological and environmental nature[19]. Thus, the threats consist in the perpetuation

[17] National Defense Strategy for 2015-2019, see fcnap.ro/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2015-2019 retrieved on 05 September 2019.

[18] See maps at ro.wikipedia.org/wiki/Transnistria#/media/fișier/South_Russia_geopolitics_2015.jpg, retrieved on 07 September 2019.

[19] National Defense Strategy for 2015-2019, see fcnap.ro/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2015-2019 retrieved on 05 September 2019.

of frozen conflicts (Transnistria, Abkhazia, South Ossetia, Nagorno-Karabakh and Ukraine), destabilizing actions represented by migration, transnational organized crime, distortions on energy markets, poor governance, terrorist actions, trafficking in weapons, drugs and human beings, corruption, ecological disasters and others[20].

Also, in all the states of the region, there are a series of political risks (amplification of corruption, an unstable internal political environment that determines the diminution of the authority of the state institutions and the accentuation of certain phenomena specific to organized crime: involvement of political and military leaders in illegal actions etc.), economic and social nature risks (crisis of states and lack or inefficiency of reforms, existence of large gaps between states, low standard of living, mass emigrants and immigrants) and security risks (separatist movements, territorial disputes, border insecurity, the existence of large quantities of weapons and ammunition, insufficient security measures)[21].

There is a gap between frozen conflicts and some of the risks that arise, especially terrorism and transnational organized crime. Maintaining the frozen latent state of these conflicts has the effect of keeping the states on whose territory they are in a state of retrogression, of stagnation from an economic, social and political point of view. These states are in course of developing, poor countries with poor population, with intense corruption and organized crime, which creates also a low level of security for the neighbouring countries[22].

There are five *"frozen"* conflicts in the Extended Black Sea Region: Transnistria, Abkhazia, South Ossetia, Nagorno-Karabakh and eastern Ukraine.

Transnistria is a separatist republic, part of the Republic of Moldova. The authorities of this separatist territory control the eastern part of the Dniester, but also the small territories located west of the river. The control of this area was lost by the Moldovan republic following a civil war in which the separatists were supported by the 14th Russian Army deployed left of the Dniester[23].

About 505,000 inhabitants lived in this area, in 2015 (compared to 730,000 in 1990), speaking Moldovan, Russian and Ukrainian. It is a territory that is not officially recognized by the UN, but only by three pseudo states: South Ossetia, Abkhazia and Karabakh (under Armenia's authority). The authorities of this republic are strongly supported by Russia, that maintains here a peacekeeping force, with a brigade-like structure, organized by battalions and with about 1,500 military personnel. All attempts to support the conflict and clarify the status of the republic have not been successful. Recently, Russian Foreign Minister, Sergei Lavrov, declared Russian

[20] *Ibidem.*

[21] Dumitru Popilevschi, *Perspective ale securității naționale la limita bazinului Mării Negre în contextul geopolitic și geostrategic al securității globale*, Chișinău, 2014.

[22] Cristina Bogzeanu, *quoted opus.*, pp. 56-57.

[23] See wikipedia.org/wiki/republica-moldoveneasca-transnistreana, retrieved on 10 September 2019.

intention of dismantling weaponry and ammunition from the huge Cobasna depot with Russian owned specialists. The Moldovan authorities stated this process could be in fact a trap, as these types of military actions should be accomplished with the participation of specialists from the 5+2 peace format countries. The necessary funds are already available following 1999 OSCE Summit, but they are blocked due to Russia's refusal to accomplish the process[24].

The negotiations carried out in 5 + 2 format (Transnistria, Moldova, Ukraine, Russia, and OSCE, respectively the USA and the EU with observer status) focused more on the socio-economic aspects and less on the political ones.

The concept of foreign policy of this separatist republic emphasizes the increased cooperation with Russia but also the necessity of obtaining and recognizing independence. As a priority, integration into the Eurasian Union is established. The relations of the Transnistrian authorities with the central ones from Chișinău are marginally addressed[25]. Given the geopolitical context in the Extended Black Sea Region and the relationship between Russia and the USA, the chances of successful negotiations for the Transnistrian problem are unlikely in the near future.

Abkhazia is a separatist territory located in north-western Georgia, declared an autonomous republic in 1962 following a civil war in which the separatists benefited from Russian military support.

South Ossetia, another separatist territory, is located in the north of Georgia, the situation of this territory in terms of relations with Tbilisi and Moscow being similar to Abkhazia. This territory was the subject of the Russian army's intervention in 2008, after which the Georgian central authorities lost control. Both territories declared their independence in 2008 following Russian intervention in Georgia, a status recognized by Russia[26].

Nagorno-Karabakh is another separatist territory located in the South Caucasus on the territory of Azerbaijan, under Armenian authority. It is inhabited by a majority Armenian, orthodox population. In this problem, the states in the area were divided in two opposite sides. On the one hand, Russia, which supports Armenia and, on the other hand, Turkey, which supports Azerbaijan. In exchange for his support, Russia has the right to have a military base on the territory of Armenia, the 102nd military base, where it has deployed aviation, artillery and radio-technical forces. The conflict has not been resolved so far, with all the negotiation sessions taking place and we consider that it is far from being resolved in the near future.

Donbas is a separatist territory located in eastern Ukraine, comprising so-called separatist republics Lugansk and Donetsk, which came under the authority

[24] Vitalie Călugăreanu, *O nouă capcană întinsă Moldovei de către Rusia*, see div.con/ro/o_noua_ capcana_intinsa_ Moldovei_de_catre_Rusia_50416132, retrieved on 05 September 2019.
[25] *Ibidem.*
[26] Cristina Bogzeanu, *quoted opus*, pp. 60-61.

of central institutions in 2014, after a war, in which the separatists were consistently supported by Russian military structures with military personnel and technique. The problems of language and political representation, subsequent to the *"Euromaidan from Kiev"* mission were the factors that generated the first separatist movements.

The military actions were stopped following political negotiations, carried out in Tbilisi in Normandy format (France, Germany, Russia, Ukraine, and representatives of the separatist republics), finalized with another treaty, known as *"Minsk 2".* The treaty established the cessation of hostilities, the withdrawal of heavy weapons at 100 km from the front line, the organization of elections in the separatist territories. None of the parties to the conflict complied with these provisions except in small part. The negotiations carried out after the conclusion of the *"Minsk 2"* treaty were not successful. We think that resolving this conflict is far from finding its solution[27]. All these frozen conflicts from the European part of the former Soviet space are located in the Extended Black Sea Region and influence all the political actors belonging to this space or with interests in the area. At the same time, the existence of the five secessionist entities gradually led to the erosion of the states from whose borders they were detached, and the consequence of this phenomenon that can be associated with the state failure, was the emergence or intensification of risks such as organized crime, transnational drug trafficking, corruption, trafficking in dangerous substances. Alarming growth has been observed in recent years for both regional and global actors, which are increasingly visible in Russia's claims in the Extended Black Sea Region[28].

ACTORS AND GEOPOLITICS OF THE REGION

The Extended Black Sea Region is far from being considered a mere temporary or peripheral breakdown that is a character of strategic importance that influences and is influenced by global actors. The region is the main transit area and one of the important sources for the energy consumed in Europe[29]. When analysing the special geopolitical importance of the Extended Black Sea Region, we had as a starting point the very special features in the region: the Crimean Peninsula, the ends of the Danube and the Bosporus and Dardanelles straits. Crimea, through its natural harbours and through its position in the Black Sea basin, has a key dominant position, assuring control over the entire region[30]. The political actors in the area are their neighbouring states along with NATO, EU and China.

[27] *Ibidem*, p. 63.
[28] Eugen B. Rumer, Jeffrey Simon, *Toward a Euro-Atlantic Strategy for the Black Sea Region*, Institute for National Strategic Studies, National Defence University, Occasional Paper no. 3, April 2006, Bucharest.
[29] Teodor Frunzeti, *Geostrategie*, Editura Centrului Tehnic-Editorial al Armatei, București, 2009, p. 55.
[30] Costantin J. Corneanu, *Interesele strategice ale României și ale Rusiei în bazinul Mării Negre*, see aesgs.ri/ Interesele strategice ale romaniei si ale rusiei in bazinul marii negre, retrieved on 11 September 2019.

The Russian Federation is the state with the largest waterfront area on the Black Sea and possesses an appreciable conventional and nuclear arsenal. The Black Sea Fleet, located mainly in the Crimean Peninsula in the Sevastopol naval base but also in the east in the Novorossiysk naval base, is the main military influence vector. This state has made great efforts to attract other states, especially China and India, in order to create an opposing NATO bloc and, simultaneously with these actions, it has taken actions to impose *"energy diplomacy"*, which aims to provide cheap energy to allies and expensive energy to its opponents, controlling its energy sources and transport routes to Europe. It has also encouraged and even actively supported separatist groups operating in states in the Extended Black Sea Region. It tried and succeeded in removing Ukraine from the path of energy corridors, strengthened relations with Turkey both politically and militarily, intensified energy cooperation with Bulgaria and Georgia and encouraged the expansion of Gazprom and Lukoil companies in the south and west of the Black Sea. The main objectives of Russia in the extended Black Sea region are, in our opinion, the following: the extension of its influence and the increase in its prestige in the region; the restoration of the military system through the restoration and development of the Black Sea fleet and of the terrestrial and aero cosmic structures; the transformation of Crimea into a military outpost that allows for projecting force in the Middle East and the Mediterranean including North Africa; counteracting the growing influence of the European Union and NATO, but also of the member states of the economic political union GUAM (Georgia, Ukraine, Azerbaijan and Moldova)[31].

Romania, a NATO member country, has a major advantage by hosting on its territory elements of the missile shield, bases on which NATO forces are stationed, and also by controlling the Danube river exits, one of the key elements of the Black Sea.

Bulgaria, a country of *"divided identity"* between East and West, although a NATO member, oscillates between the mirage of opportunities ensured by EU and NATO membership and the tradition of historical relations with Russia. Although it has on its territory military bases that host NATO troops, especially belonging to the USA, and has encouraged GUAM actions, Bulgaria granted advantageous facilities to Russian companies Gazprom and Lukoil but also to other Russian companies operating in the energy field, including the nuclear field. Together with Romania, it is the eastern border of the EU[32].

Turkey, a NATO member state with geopolitical pivot value, controls the Bosporus and Dardanelles straits that control the maritime access route from the Black Sea and the Mediterranean and the planetary ocean. It ensures growing influence

[31] Marius Roșu, *Political Considerations regarding the Black Sea Extended Area*, PhD thesis, Bucharest, 2015.
[32] *Ibidem*, pp. 53-54, 62.

in the Middle East and the South Caucasus and it has also re-established relations with Russia, especially after the failed military coup, having chosen to purchase S-400 anti-aircraft defence systems from Russia and also to manufacture assembly within the complex military program of Russian weapons systems. The cooperation with Russia has also been intensified in the energy field by the construction of the Russian Turkish Stream gas pipeline by Gazprom and the Akkuyuk nuclear centre, by the Russian company Rosatom.

The United States as a NATO leader has shown increased interest in the region after 2001, with the launch of the Afghanistan anti-terrorist campaign, and especially after 2008 Georgian war and the annexation of the Crimean Peninsula in 2014. The USA promotes the internationalization of the Bosporus and Dardanelles straits[33] status, the resolution of frozen conflicts, the intensification of the cooperation in the region, the fight against risks and especially against the arms trafficking and cross-border crime[34].

Another important player in the Extended Black Sea Region is the *European Union*, which reached the Black Sea in 2007, with Romania and Bulgaria membership of the Union. The involvement of the EU in the Extended Black Sea Region has been marked, during the past decade, in the context of the energy tensions with Russia, by the projects of alternative routes. In 2008, it initiated the project *"Black Sea Synergy"* within the European Neighbourhood Policy, which includes 10 states.

Another important player in the region is *Ukraine*, a state with a geopolitical pivot role in the extended Black Sea region, which has been subject to obvious aggression by Russia after 2014. Referring to this role of geopolitical pivot of Ukraine, the renowned Zbigniew Brzezinski mentioned that *"Russia without Ukraine ceases to be a Eurasian Empire"*. Geographically, Ukraine has three distinct regions, respectively Western Ukraine, Eastern Ukraine, and Central Ukraine. The Crimean Peninsula, which was annexed to Russia in 2015, constitutes the fourth region, after USSR President Nikita Khrushchev signed in 1954 the decree to attach this territory to the Soviet Union. In his paper *"Clash of Civilizations"*, Huntington states that Ukraine represents a torn territory between the Russian-speaking east and the nationalist west. By annexing Crimea, Russia has achieved a true strategic control point for the entire extended Black Sea region through the military infrastructure represented by the exceptional Sevastopol naval military base and also by the air and land bases in the area. Through the Eastern Civil War in Lugansk and Donetsk, Ukraine loses control over the richest region in the country. Minsk agreement which stopped hostilities on the border between the parties involved in the conflict did not change Ukraine's borders but we can say that a new border has been drawn

[33] *Ibidem*, p. 55.
[34] Eugen B. Rumer, Jeffrey Simon, *quoted opus*.

within the state. This newly created border is monitored and observed by the OSCE, an organization in which Russia has a veto right. Basically, by this move to Minsk, Russia has created a buffer zone necessary for the creation of the *"sanitary cordon"* in the Euro-Atlantic region and the close vicinity[35].

Georgia and Moldova are states in the Extended Black Sea Region that are similar in some respects in terms of geopolitics. The size of the two states is relatively small, with populations of five and seven million inhabitants, and within their territory are frozen conflicts, sources of insecurity. Also, both states have complex relations with Russia, do not have control over part of the territory and are dependent on Russian energy resources, primarily gas and partly energy[36].

Armenia is one of the actors in the vast Black Sea region and a strategic partner of Russia. In spite of this, Armenia is subjected to abusive treatment by the strategic partner, under the conditions in which it has agreed to give up the economy for a low price for oil and natural gas. For Russia, Armenia represents a strategic stake in the fact that it bought its energy production and transport infrastructure (largely built with Iranian capital) thus blocking the use of alternative transport of Iranian gas or gas from Central Asia to Europe. Also, all the companies that constituted profitable businesses, especially in the field of communications, were taken over at very low prices[37]. Through this economic vector, Russia can control and impose the geopolitical evolution of Armenia.

Azerbaijan is the most important energy player in the South Caucasus and is subjected to the others in the extended Black Sea region, to the actions of Russia that has transformed its energy policy into an instrument of domestic policy. Through these actions, Azerbaijan is subjected to a commercial blackmail to accept the price of natural gas and oil imposed by Russia. But this state resisted the commercial blackmail, through the decisions of its president, declaring *"I cannot allow this. Azerbaijan is no longer the kind of state to be forced into something"*[38].

While the international community was attentive to Russia's strategic actions, an actor who does not belong to the Euro-Atlantic but to Asia has begun to expand insidiously and subtly in the Black Sea region. This actor is China. Taking as its starting point the promotion of its own interests, China has identified considerable opportunities in the region which is a constituent part of the trans-Eurasian concept *"one belt, one road"*. The first part of the ambitious Trans-Caspian International Transport Route (TCITR) project linking China to Kazakhstan, Azerbaijan, Armenia, Georgia and further into Europe, was completed in August 2015. This route includes

[35] Marius Roșu, *quoted opus* pp. 68-69.
[36] *Ibidem*, pp.70-71.
[37] Iulian Chifu, Lavinia-Florentina Diaconu, *Russian Federation Energy Policy*, see cpc-ew.ro/pdfs/securitatea-in regiune-marpdf., retrieved on 06 September 2019.
[38] *Ibidem.*

4,000 kilometres of railway with the transport capacity that in 2020 will have 13.5 million tons of goods and 300 thousand containers[39].

Currently trade between China and the EU exceeds 1.5 billion Euros a day. In contrast to Russia, China saw the modernization and Euro-Atlantic integration of the former Soviet republics as business opportunities with a presumed win-win result.

Figure no. 4: Trans-Caspian International Route[40]

Regardless of what China could plan in the immediate vicinity, it distanced itself from Russia and its military adventures. However, in the current context, naval military action in the Extended Black Sea Region has also intensified. 2017 is the year representing the first time in history when China has participated in a naval exercise in the Black Sea in cooperation with Russia. At the same time, China initiated a deep sea port development project in Anaklia, Georgia, as a transit point on TCITR, which will reduce all costs and ensure the exploitation of regional economic development opportunities[41]. The construction and operation of this bridge was entrusted to an international consortium in 2016, made up of companies from the United States, the United Kingdom, Georgia, Kazakhstan and Bulgaria. The plans foresee that this can become operational in 2020.

[39] Ganibov, *A2AD*, in *Eurasia Daily Monitor*, Jamestown Foundation, Washington DC, issue 75.
[40] See https://clubferoviar.ro/forumul-railway-pro-ruta-trans-caspica-de-transport-international-va-folosi-legatura-astara/
[41] See ankaliadevelopment.com, retrieved on 09 September 2019.

Figure no. 5: Anaklia, GEORGIA, transition area TCITR

In the Extended Black Sea Region, there are complex geopolitical evolutions, focused on conflict points, related to the reconstruction of the nations in the region or to the territorial or ethnic disputes that followed the dissolution of the Soviet Union[42]. The tensions that are found in the region have a very high potential for contamination of the near neighbourhood, being motivated by ethnic, religious or territorial reasons. The related approaches generated by solving the problems imposed by the geopolitics of the borders have been and are flagrantly violated by Russia. Its interest is not to solve the problem, but to keep the outbreaks of conflict in a latent state and to control the whole (sovereign states or areas of interest) by establishing control over a part (conflict zone), such as in eastern Ukraine, Transnistria, Abkhazia, South Ossetia or Nagorno Karabakh. The analysis of these conflicts leads to the conclusion that behind all of them are projects inspired by Russia, through which violent or political conflict actions can be activated or deactivated, depending on Russian strategic interests.

By *"freezing"* these conflicts, Russia has a considerable capacity to manipulate, influence and control directly or through third parties, internal developments, conflicts in *"host"* states or regionally[43]. The regimes established in these separatist territories, these state entities not recognized by the international community, constitute excellent levers of Russia's geopolitical actions. Russia's delay in resolving these conflicts is favourable to it, while the defrosting attempt is intended to gain even more benefits[44].

[42] Marius Roşu, *quoted opus*.
[43] *Ibidem.*
[44] In Transnistria, Russia is announcing intention to withdraw its ammunition, resuming negotiations between the parties representing an attempt by Russia to consolidate the regime established by President Igor Dodon.

In this context, the geopolitical processes in the Extended Black Sea Region are influenced by the location of the energy resources and the difficulties that their transport entails to the beneficiary. The *"frozen conflicts"* make the exploitation and transport of energy resources a security issue. Complementary risks or arising from *"frozen conflicts"* may deter future investments. The energy resources and their transport, the political evolutions and the security environment in a continuous dynamic, significantly influence the foreign policy of all actors in the Extended Black Sea Region[45]. On the one hand, Russia is trying to gain economic benefits by exploiting its huge reserves of natural resources, by controlling the transport of oil from the Caspian Sea through the Black Sea, to Turkey and Europe, to some extent, setting the terms and conditions for how the gas market in Europe works.

For the United States of America, the Extended Black Sea Region is an area of geopolitical importance due to the existence of energy resources, the security of their extraction and transport routes, the political developments, the dynamics of the borders and the security environment.

The energy resources of the Black and Caspian Sea area represent huge stakes for the EU, even when a consortium of companies from Western EU member states and Russia build the Nord Stream 2, which increases the transport capacity between Russia and Germany on the route north to 110 million cubic meters per year. This has the effect of transforming Germany into an energy hub for Western European countries and increasing their dependence on Russian gas. Another conclusion can be drawn, even under the sanctions imposed by the EU on Russia following the annexation of Crimea and involvement in the war in eastern Ukraine, when the interests of large Western companies are at stake, democratic values matter less. This aspect is also confirmed by the contradictory discussions held by the leaders of the G7 group of the most powerful industrialized states in the world, to reinstate Russia in organization.

The European Union as an organization is developing strategies to reduce its dependence on Russian energy resources. As the consumption of energy resources increases this dependence deepens. The EU needs access to diversified energy sources, alternative supply routes and strategic access to Central Asian sources, given that its natural gas consumption will double (it will reach 400 million cubic meters per year)[46]. But Russia does not have the capacity to supply all the resources it needs even from its own resources, even when it makes

[45] Tracey C. German, *Corridor of Power: The Caucasus and Energy Security*, in Caucasian Review of Internal Affairs, Spring 2008, pp. 64-72.
[46] See http:www.gepoitic.ro pdf, retrieved on 16 September 2019.

massive investments in its own infrastructure to increase production. On the other hand, Azerbaijan and Central Asian states, Kazakhstan Turkmenistan and Uzbekistan, have great potential for untapped oil and natural gas. Given the sanctions imposed on Russia, the monopoly it has on the transport of energy resources from Central Asia and Azerbaijan and Russia's desire to exclude Ukraine from the energy transport routes, the question arises related to reaching the beneficiaries. Part of the answer was found by creating Nordic Nord Stream routes 1 and 2 and the new Blue Stream to supply gas to Turkey.

Given that only part of the production of the gases transported through these last two pipelines is used on the Turkish market, Russia desires to own the monopoly of the distribution of energy resources on the European market and to use this domination for political purposes.

Figure no. 6: Existing and planned natural gas pipelines to Europe[47]

The transport monopoly is also reinforced by the fact that the status of the Caspian Sea, the first in history, signed in 2018 by all neighbouring states, regulates the construction of underwater pipes, which require the Central Asian countries to use in particular the Russian transport infrastructure. Thus, the key to Russia's security strategy in the Extended Black Sea Region is to ensure the proper transport of energy resources from Central Asia and the Caucasus by applying energy blackmail to both producers and consumers.

The EU is looking for alternatives to increasing dependence on Russian gas and has thus achieved the INOGATE project, which involves the construction of pipelines that will connect gas producers in the Caspian region to Europe. This process is already underway by integrating European gas transmission networks, on the one

[47] See https://www.enpg.ro/turcia-da-sah-mat-eu, retrieved on10.09.2019.

hand, and building a new transport infrastructure that will connect Azerbaijan with Turkey, on the other hand. In its realization, there are numerous problems especially created by the Turkmen-Azerbaijani dispute regarding the creation of a trans-Caspian pipeline and the exploitation of resources in the Caspian Sea.

The geopolitics of power relations in the Extended Black Sea Region is particularly complex due to the security dilemma between the USA and Russia, the conflict in eastern Ukraine, the multiannual planning in the area of military exercises as well as the balance of power in the region[48].

The security dilemma in the extended Black Sea region is created by Russia, which seeks to strengthen its security situation by threatening actions against the territorial security and integrity of Moldova, Ukraine and the South Caucasus states, but also towards the energy security of the EU.

The geopolitics of military shelters in the Extended Black Sea Region is amplified especially by the events in eastern Ukraine having a major impact on the balance of power and security architecture in the region. The key to the politics of power relations in the region is the relationship between NATO, and especially the USA, and Russia. At all the NATO summits, the agenda also included the security situation in the Extended Black Sea Region, the problems it entails, and the necessary measures. NATO-Russia and USA-Russia bilateral cooperation frameworks have been suspended, only those at the highest level are maintained. The USA, in particular, as well as other important NATO member states have increased presence on the south-eastern flank of NATO which subscribes to the extended Black Sea region including Ukraine and Georgia. BLACKSEAFOR and Black Sea Harmony regional cooperation frameworks were also suspended. The Black Sea economic cooperation organization continued its activity, but with a lower intensity. In the same parameters was the activity of the Black Sea cooperation forum. After the annexation of Crimea, there was no further activity of regional initiatives aimed at securing maritime freight routes and jointly carrying out naval interdiction exercises with Russia, dredging of maritime mines and regional military cooperation between the maritime fleets of the Black Sea neighbouring states.

The NATO paradigm of security in large areas of the Black Sea has been modified in particular by the 2014 Wales Summit documents, in the context of annexing Crimea and of the events in eastern Ukraine. In the US perspective, in the context of the conflict in eastern Ukraine, Germany was considered a crisis manager state, assigning its role to be the interface between the West and Russia as a result of the trust capital that German Chancellor Angela Merkel enjoys in Moscow. In this capacity, Germany has led the Diplomatic Dialogue between the West and Russia. In the meantime, diplomatic relations have suffered nuances, even in the views

[48] Marius Roșu, *quoted opus*, pp.106-109.

of the leaders of the Euro-Atlantic bloc, that it would be time for Russia to be repressed in the G8 and would have the effect of including the withdrawal of sanctions imposed on Russia starting 2014 after the annexation of Crimea. Probably, analysing the latest events, the latest positions of European and US leaders this time is not too far off[49]. Another very important aspect that must be considered when referring to the situation in the Extended Black Sea Region is that of the relations between Turkey and NATO and the USA in particular. These relations suffered as a result of Turkey's decision to purchase S-400 anti-aircraft defence systems from Russia. The USA in particular appreciates that these systems cannot be interoperable with those of NATO member states and endanger collective security. Following this decision, the USA decided to exclude Turkey from the F-35 multirole aircraft programme. Under these conditions, Turkey has increasingly turned to military cooperation that has become increasingly widespread with Russia. Thus, it assembles in his own production a series of Russian armament systems, is oriented towards the purchase of Russian fighter planes SU-35 and even analyses the Russian offer for the acquisition of SU-57 latest generation aircraft.

There are voices in the US capital, especially in the last year, relating to excluding Turkey from NATO. The Turkish Permanent Representative to NATO appreciates that it is a huge mistake to include the Alliance in the issue of arms procurement of his country which damages the cohesion of the Allies.

The negative evolution of Turkey's relations with the USA and NATO is generated by other issues such as involvement in solving the Syrian crisis, in a format that does not include the USA and NATO, the support given to Iran at the expense of relations with Saudi Arabia and its Gulf partners and the involvement in the crisis in Venezuela by supporting President Nicolas Maduro[50].

Ukraine has also influenced the rhetoric on NATO adaptive European approach to the ballistic missile defence system (BRD), which is an essential element of the European security architecture, and its development has influenced and continues to influence disarmament negotiations between Russia and the USA. NATO insists that the system is not offensive and is not aimed at Russia, its purpose being the defence against missiles launched in the Middle East. This system enjoys strong support from the states on the south-eastern flank of the Alliance, signifying the United States of America firm commitment to the old continent.

In this context, the consolidation of NATO military forces in the south-eastern flank of the Alliance is perceived by Russia as a direct threat. Consequently, especially after 2014, Russia has developed an ambitious programme with its military structures in the Extended Black Sea Region.

[49] *Ibidem*, pp. 104-108.
[50] See monitorulapararii.ro/evenimente-poitico-miitare-nato-ue-iunie-1-17355, retrieved on 9 September 2019.

RUSSIA MILITARIZATION OF THE BLACK SEA

Russia is paying close attention to the vast Black Sea region. This interest was clearly expressed in February 2007 at the security conference in Munich when the Russian President Vladimir Putin declared transiently that he was no longer willing to tolerate what he called the intrusion of NATO in the areas of special interest of Russia. In the same year, measures were taken to revitalize the Russian military forces layout in the Black Sea basin, including in the Southern Caucasus states. Russian analysts appreciate that this decision had the role of a beginning of an era of confrontations, in which Russia is based only on a different set of values that are guided by the traditional *"aspirations for justice beyond formal laws and rules"* and the desire to defend national interests through the use of force[51]. The first test was the war in Georgia, after which the conclusion of the Russian military analysts was that military capabilities specific to all categories of modern and performing forces are needed. It was the beginning of an ambitious project to develop military capabilities in the area, which included in particular the development and modernization of the Black Sea fleet, the establishment of the military port of Novorossiysk and the air capabilities associated with the fleet. The annexation of Crimea in March 2014 gave Russia a clear geostrategic advantage, ensuring the possibility of transforming the peninsula into a very strong naval and air bastion and the creation of an anti-access area (A2AD). This system is a challenge and a threat to NATO's eastern flanks and even to the whole Europe as a result of its potential for deterrence[52].

Russia's strategic forces layout in the Black Sea has two components. The eastern one, based mainly on fleets located in Novorossiysk, in the naval bases in the eastern Black Sea and in Abkhazia, South Ossetia and Armenia, has the mission to maintain influence in the Caucasus region. The Crimean one, whose mission is to control navigation in the Black Sea region, to protect communications lines and energy transport routes, to intimidate Bulgaria, Romania and Turkey and to prohibit the access of NATO naval forces to the Black Sea basin, outside the restrictions imposed by the Montreux Convention[53].

The extent and speed of modernization and transformation actions of the Russian military layout in the region, especially in Crimea, including the road, naval, airport infrastructure, the arrangement and modernization of ground forces, aviation and air defence units as well as the modernization of naval forces is impressive.

[51] New Strategy Centre, *quoted opus*, pp. 5-6.
[52] George Vișan, Octavian Mauer, *The Emerging Access-Denial Challenge for NATO's Eastern Flank*, in *The Black Sea in Access Denial Age*, Romanian Energy Centre, special report created with NATO support, Bucharest, January 2019, p. 19. More on New Strategy Centre, *quoted opus*, pp. 5-6.
[53] *Ibidem*.

In recent years three highways have been built that cross the peninsula from west to east and from south to north, a road bridge has been completed over the Kerch Strait, and a railway bridge is about to be completed. Also, both civil and military airports have been modernized. Particular attention was paid to the harbour infrastructure, capable of accommodating the main structures of the Black Sea fleet, which also provides the vessels that make up the permanent Russian naval group in the eastern Mediterranean, whose main base is Tartus, in Syria. In the composition of the Black Sea fleet, the second Black Sea fleet as of importance (after the North fleet) within the Russian naval forces, there are six Krivak class frigates (five equipped with Kalibr rocket launching facilities), six kilo-class submarines and six corvettes carrying Kalibr rockets[54]. To this, a large number of patrol boats and vessels are added. New ships are planned to enter the naval force, the attention it enjoys being confirmed by the statement of its commander, Vice Admiral Alexander Moisuv, this year: *"Russia's history has confirmed: without a strong army there is no powerful state. The Russian fleet in the Black Sea has been, is and will be a guarantor of Crimea security and the entire region. The current state of the fleet does not raise doubts in its ability to carry out such tasks"*[55].

The Russian strategy in the extended Black Sea region combines information and electronic security, tactical and strategic air operations, an integrated anti-aircraft defence system that supports naval superiority in which submarines play a key role.

In the field of information security, there has been a huge development in recent years. An automated jamming complex of *"Murmansk BN"* type radio communications with a range of 3,000 km was deployed in Crimea, a modernized early warning radar *"Voronej-SM"*, also with wide range, radio equipment and TU capable of transmitting in the southern and eastern regions of Ukraine, *"NEBO"* electronic warfare systems. An aviation division with 5 regiments was set up, having Su-35 Su-34, Su-27, Su-24 aircraft as well as different types of helicopters with different destinations and 22 long-range bombers, TU-22M3. Crimea's antiaircraft defence system has been upgraded to include S-300, S-400 long range anti-missile rocket systems, medium range *"BUK"* systems and short range *"Pantsir S1"* systems.

There are indicators that the R 500 (Iskander) cruise missile systems are also located on the peninsula. The anti-ship system is equipped with *"BAL"* and *"BASTION"* rocket systems.

[54] New Strategy Centre, *quoted opus*, p. 7.

[55] See g4media.ro/flota-rusa-din-marea-neagra-se-intareste-cu-13-nave-echipate-cu-rachete-de-croaziera-kalibr.html, retrieved on 01 September 2019.

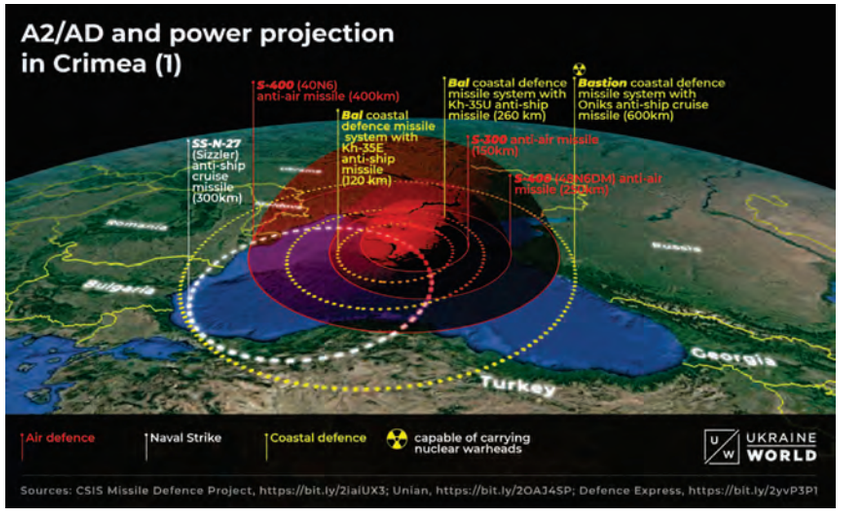


Figure no. 7: Crimea's defence system[56]

All of these actions carried out by Russia in the Extended Black Sea Region for the reconfiguration and development of the military layout underline its clear determination to transform Crimea into an A2-AD area with offensive character and lead to the conclusion that the neighbouring NATO member states are considered as a regional threat aimed at blocking and encircling Russia. Crimea is a pivot of Russia's eastern device that can be called the steel arch.

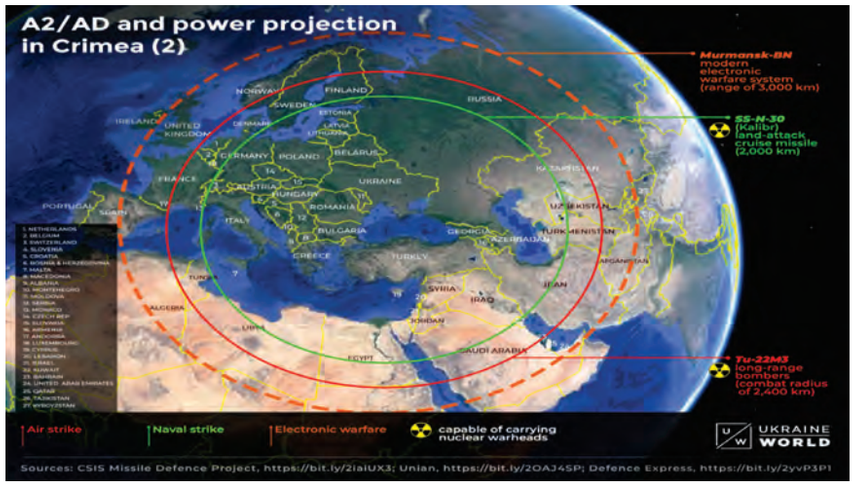


Figure no. 8: Russian Western defence projection called "The Steel Arch"[57].

[56] *CSIS Missile Defense Project,* see https://bit.ly/2iaiUX3, retrieved on 10 September 2019.

[57] *Ibidem.*

Out of all Black Sea neighbouring states only Turkey has consistent naval and air forces[58]. Recently, Turkey announced its intention to build a new naval base in the vicinity of Trabzon. However, Russia's fears about Turkey are diminishing due to growing closer relations between the two states.

CONCLUSIONS

The complexity of the Extended Black Sea Region, its characteristics and the processes the area is subject to, have led to geopolitical developments that generated strategic actions to gain a role in the region as significant as possible. Massive imbalances and unpredictable developments have marked the last few years.

According to the latest regional developments, Russia will use the energy weapon to impose expansionary political will. Moreover, Russia will not hesitate to use military force, for which it has developed a formidable military forces layout in the region. We can see that the problems in the Extended Black Sea Region are on the agenda of all European state leaders, influencing the courses of action throughout Europe, the Middle East and Central Asia.

In our opinion, there is a need for a change in the NATO and the USA approach to the situation in Ukraine, Syria and Iraq, as well as to the frozen conflicts in the South Caucasus, an approach in which Romania and Turkey can be important actors. Thus, the new strategy must involve an integrated approach to the area and a guarantee from the USA to its allies in the region.

Security issues in the Extended Black Sea Region and the Middle East area need to be integrated as belonging to the same Black Sea security complex, with two distinct problems.

The importance of the Extended Black Sea Region is a serious issue, being explicitly confirmed by the content of the final documents of the NATO and EU summits, as well as the security strategies of the regional actors.

The solution of the problems encountered in the Extended Black Sea Region is not Russia's isolation but negotiations. In this context, Romania represents an anchor of stability on the south-eastern flank of NATO.

BIBLIOGRAPHY

1. Cristina Bogzeanu, *Evoluția mediului de securitate în zona extinsă a Mării Negre și influența acesteia asupra configurării forțelor navale ale României pe termen mediu și lung*, Editura Universității Naționale de Apărare, *"Carol I"*, București, 2012.

[58] New Strategy Centre, *quoted opus*, p. 7.

2. Barry Buzan, Ole Waever, *Security, a New Framework for Analysis*, CA Publishing, Cluj-Napoca, 2011.
3. Petrică-Lucian Foca, Vasile Cerbu, *Romania, a Country in the Middle of a Perfect Storm,* in *Gândirea Militară Românească*, no. 4/2016.
4. Teodor Frunzeti, *Geostrategie*, Editura Centrului Tehnic-Editorial al Armatei, București, 2009.
5. Dominic Lieven, *Dilemmas of Empire 1850-1918, Power, Territory, Identity*, in Journal of Contemporary History, vol. 34, no. 2, April 1999.
6. Raluca Niga-Bestiliu, *International Law*, All Publishing Bucharest, 1998.
7. Eugen B. Rumer, Jeffrey Simon, Toward a Euro-Atlantic Strategy for the Black Sea Region, Institute for National Strategic Studies, National Defence University, Bucharest, 2016.
8. German C. Tracey, *Corridor of Power: the Caucasus and Energy Security*, in Caucasian Review of International Affairs, vol. 2, Spring 2008.

WEBOGRAPHY

1. https://newstrategycenter.ro>wp-content>uploads>2016/049… iunie_2016_1.pdf
2. https://ier.gov.ro/wp-content/uploads/publicații/spos_2009_4_ro.pdf
3. http://www.facebook.com/notes/iulian/chifu-istoria-unui-concept-de-securitate-în-regiunea-extinsă-a-Mărtii-Negre/
4. http://titulescu.eu/2011/05/zona_extinsa_a_marii_negre_povara_sau_sansa_pentru_riverani/
5. http://ibn.idsi.md/sites/default/files.imag_file/Amenințăti_și_vulnerabilități_la_adresa_securități/_o_pdf
6. http//: www.maps.com
7. https://www.unap.ro/ro/doctorat/teze_doctorat/2016_ianuarie/ROȘU-MARIUS.pdf.
8. https://revistapolis.ro/falia-strtegică-marea-neagră-marea-baltică/
9. https://ro.wikipedia.org/wiki/Transnistria#/media/fișier/South_Russia_geopolitics_2015.jpg
10. https://iran-resist.org/article 2357
11. https://fcnap.ro/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2015-2019/
12. https://www.ro.wikipedia.org/wiki/Republica_Moldoveneasca_Transnistreana
13. https://div.con/ro/o_noua_capcana_intinsa_Moldovei_de_catre_Rusia_50416132
14. https://g4media.ro/flota-rusa-din-marea-neagra-se-intareste-cu-13-nave-echipate-cu-rachete-de-croaziera-kalibr.html
15. https://monitorulapararii.ro/evenimente-politico-militare-nato-ue-iunie-1-17355;
16. https://dantomozei.ro/2017/05/08/china-dezvolta-drumul-matasii-feroviar-europa-asia;
17. https://www/geopolitic.ro/R%20Geo/2019.pdf
18. https://aesgs.ro/interesele-strategice-ale-romaniei-și-rusiei-in-bazinul-marii-negre;
19. https://cpc-ew.ro/pdfs/securitatea_in_regiunea_mar.pdf
20. https://www.enpg.ro/turcia-da-sah-mat-eu

INNOVATION, PROTECTION OF A MILITARY CHARACTER INFORMATION GUARANTEE IN THE INFORMATION SOCIETY BASED ON TECHNOLOGIES

Lucian SCÎRTOCEA

PhD Candidate, "Carol I" National Defence University, Bucharest

The information society based on technologies, as a phenomenon and consequence of globalization, favours the extension of threats and vulnerabilities while generating new means and ways to combat them. The developments in information technology offer an unprecedented amplification of human abilities to access critical information that governs any field of activity. In the context of the full NATO integration, the Romanian Armed Forces undergo profound political, economic, social and cultural transformations. This set of transformations affects the life of each of us. Therefore, "innovation", as such, could become a "weapon" to defend against risks, anticipating the development of new vulnerabilities that will surely appear in the society of the coming decades.

In this paper, I will summarize the presentation of some innovative ideas that may have the effect of diminishing the vulnerability of military information transmitted in the electronic environment under the conditions of adopting a new development doctrine in Romania, the one of the information society based on knowledge, training and education.

Keywords: innovation, operating environment, data security, vulnerability, networks.

INTRODUCTION

11 September 2001. Terrorists hijacked planes and hit twin towers at the World Trade Center in New York, and the Pentagon in Washington. Before assessing human losses or identifying terrorists, experts from all over the USA began to make assumptions that an attack, a cyber-attack, would follow.

"Terrorists have attacked our major political and financial centers" security consultant Donn Parker stated for USA Today. He added that *"The next logical step would be to attack our computer infrastructure"*. For example, terrorists could make things worse by disrupting 911 communications in New York during an emergency. Thus, the Internet and critical computer infrastructure have become vulnerable as the Pentagon has for many years warned that a cyber- attack can be just as dangerous as a kinetic attack. The enemies of a state could use computers to leave the nation without electricity, telephony, air traffic control and without the Internet.

What has changed in contemporary man is the way the world has linked through information. Information has always been important to society both in peace and at war.

FROM THE INDUSTRY-BASED SOCIETY TO THE INFORMATION-BASED SOCIETY

As technology has evolved, and innovation plays an important role in this regard, weapons and communications have also developed. Intercepting the messages transmitted by commanders on the battlefield and finding their orders can give the enemy an advantage. From the beginning of the world, knowing when and where the enemy will attack makes the difference between winning and losing the battle, between life and death. The information revolution is similar to the industrial revolution from the point of view of the incredible changes brought to communications, work and people's lives. The information revolution has transformed the world from an industrialized society into an information-based society.

The emergence of the Internet, due to an intense scientific research in the military, has made distance no longer important as people began to communicate from one side of the globe to the other.

At the same time, it is well known that whoever has the information has power and we can supplement that whoever protects the information has wisdom.

Any material published under the title *"Information Protection and Security ..."*, upon closer examination, is quite confusing, since in the society we live in it could be more easily talked about data insecurity than about their security. Moreover, there is no question that sometimes too much computerization could be harmful. When users became aware of the benefits of computers, several organizational entities triggered a huge process of information retrofitting, reporting with satisfaction what massive investments they made in education, research and computing.

There are also cases in which computerization has become *"a fashion"*, without taking into account the risks of this process.

The military structures, however, have proved to be aware of the risks associated with the dependence on computer networks and harmonized the legislation in correlation with the new security challenges. Thus, according to the national legislation and the special departmental regulations, each military structure (organization) must take all measures to ensure the necessary information and to organize the information systems that allow to fulfil its missions (objectives), providing legal users with truthful, relevant, timely information (almost in real time) and as complete as possible.

The particular importance of information for the successful execution of command and control, therefore of the management processes in general, has generated the necessity to ensure its protection, especially in the case of the information classified in all its phases of existence.

In the combat space, through the information defence operations[1] the protection of information for the combined forces, command and control systems, as well as the information systems held by them is ensured. They allow commanders to have a common operational picture based not only on the military perspective, but also on the consideration of non-military factors that can affect the situation, which can ensure its complete understanding. At the same time with the mentioned protection actions, using the resources of creativity available, actions of misinformation of the potential adversaries regarding the information held about them must be organized. In general, the concept of information protection is increasingly being replaced by the one of information security that we will continue to use.

Internationally, information security rules[2] represent the minimum requirements and parameters that must be met by the security mechanisms in order for them to be considered accepted, approved or authorized and certified. The norms deal with different aspects of the responsibilities of the information holder, of their classification and description, of the evolution of dangers and risks,

[1] Information operations are continuous military actions in the information environment that ensure the improvement and protection of the abilities of the Allied forces for gathering, processing, dissemination and action with information for gaining operational advantages, FM 100-6, Information Operation, 1996, p. 64.

[2] Gheorghe Ilie, Ion Stoian, Viorel Ciobanu, *Securitatea informațiilor*, Editura Militară, București, 1996, p. 64.

of the organization and evaluation of the risks arising from what the information protection means. The general elements regarding the management of information security are established by the series of ISO/IEC 27000 standards, a greater applicability having the standards ISO 27001, 27002, 27005, which also include references to the management of the information security risk considered a component thereof.

Also, if we refer to NATO, the military regulations and manuals held by the armed forces of the Allied countries include measures to protect information against the dangers and threats specific to the information age.

In our country, a special law[3] on the protection of classified information has been developed for this purpose, whose main objectives are:

- protection of classified information[4] against spying, compromising or unauthorized access, altering or modifying their content, as well as against unauthorized sabotage or destruction;
- achievement of security of information systems and transmission of classified information.

The measures deriving from the application of the law are intended:

- to prevent unauthorized access to classified information;
- to identify the circumstances, as well as the persons who, by their actions, may endanger the security of the classified information;
- to guarantee that the classified information is distributed exclusively to the persons authorized, according to the law, to know it;
- to ensure the physical protection of the information, as well as the personnel necessary for the security of the classified information.

INFORMATION SECURITY – DEFINITION AND CHARACTERISTICS

The field of information security is disputed at the moment by at least four categories of specialists, belonging to the following areas: system security, computer systems development, legal – concerned with the difficulties of pronouncing in the cases of information piracy – and penetration of security systems. Regardless of the domain to which the specialists belong, they recognize the complexity, multidimensionality and dynamics of information security.

[3] *Law no. 182* of 12.04.2002, regarding the protection of classified information, published in the Official Gazette no. 248/2002.

[4] *Classified information* is information, data, documents of interest to national security, which, due to the levels of importance and consequences that may occur as a result of unauthorized disclosure or dissemination, must be protected. The secretization classes are: state secrets and service secrets. State secret information is information that concerns the national security through which disclosure may harm the security and defense of the country, and secret service information is information whose disclosure is likely to cause harm to a legal person under public or private law. The levels of secrecy that are attributed to the information classified in the state secret class are: strictly secret of special importance, strictly secret and secret [Law no.182 / 2002].

There are two tendencies in this competition of opinions: a global one, which tries to deal with the problem completely and exhaustively, and the selective and pragmatic one, offering practical "recipes" for security, adapted to the operational needs.

Therefore, the field of information security represents a complex of legal, scientific, economic, organizational, informational and technical measures and countermeasures capable of securing the secrecy, semantic and physical integrity of information aggregated to a system and the dynamics of their transformations against crimes, exceptions, errors or mistakes, having an intended or accidental character, within the limit of a risk assumed and with a consumption of human and material resources resulting from a minimum (optimal) cost allocated to fulfil the mission of the system.

By this definition, the following characteristics are attributed to the field of information security:

- complexity, reciprocity and active character (measures – countermeasures);
- multidimensionality: legal, scientific, economic, organizational, informational and technical;
- specialization of the objective: ensuring the secret and integrity of the information;
- dynamics, resulting from: the dynamics of the objective, the perish ability of the legal provisions, the improvement and development of science, the economic evolution, the need for organizational updating, the semantic, logical and physical transformations of information;
- the multitude and the complex character of the attacks (crimes, exceptions, errors or mistakes);
- transparency in the field of use;
- selectivity of security, conditioned by the risk assumed;
- the resource consumer character;
- cybernetic manifestation, adaptable, perfectible and open.

The cybernetic model of this field highlights: the dynamism, tolerance and regulation conditioned by the risk assumed and the cost of the mission, as well as the double destination of the countermeasures: internal and external.

The security of information and information systems[5] is a component of the security of the information society and consists in the protection against the unauthorized access of the opponent to equipment or for its modification of the (classified) information during the storage and processing in computers or transmission (circulation). It also provides protection against denial of services of authorized users (Denial of Service – DoS) and favours the provision of services

[5] FM 100-6, *Information Operations, Glossary, ibidem.*

by unauthorized users (of the adversary). It includes the necessary measures for the protection of the own decision-making bodies against the information operations of the adversary, detection of intrusions and control of the threats.

Security processes include innovative methods used for the implementation and assurance of security objectives being designed for identifying, measuring, leading (managing) and controlling the security risk of information. It represents the likelihood that they will face the danger of affecting confidentiality, integrity or availability arising from the possibility that a threat may be realized by exploiting a vulnerability.

Under modern conditions, the security of information and information systems is a priority task of commanders and other persons involved in command and control, information and decision-making activities. Information security measures have always been important, but at present they are of particular importance due to the wide development of information and communication technology. Here again, innovation plays a very important role. As the level of technological development of computer-based systems increases, we will witness a major increase, at least in proportion, of the level of security risk and implicitly of the related system losses.

The main features of information security are:

- information security aims to protect the confidentiality, integrity and availability of information through a variety of procedural, technical and administrative control actions;
- security measures should detect threats and risks in a timely manner, establishing on this basis the directions and areas in which to act, have an anticipatory and predictive character[6], and the response to overcome the hostile actions of opponents in the information field;
- the extent of security measures is directly proportional to the level of development and use of information and communication technology, so that the higher the vulnerabilities and the information threats, the more important they are;
- the level of information security is higher as the importance of the operations (military actions) is higher, and the military structures involved do not have a higher hierarchical level and require a more complex command and control system based on a wide information assurance;
- the more equipped the information systems are, with technical equipment of communications and computers, the more security measures are more important and need to be applied with more consistency;

[6] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale militare, servicii și tehnologie*, Editura Universității Naționale de Apărare *"Carol I"*, București, 2010, pp. 250-252.

- information security depends on the professional training, competence and loyalty of the personnel who ensure the functioning of the information system as well as the consistency of applying administrative measures to protect the information;
- the security methods, techniques and modules used should not affect the information compatibility and interoperability of the allied military structures that carry out joint actions.

For the fulfilment of the provided characteristics, the protection of information has a developed information assurance[7] that includes the actions destined for the security (protection) and the defence of the information (especially of the classified ones) and the information systems, in order to ensure the availability, the integrity, the authenticity, the confidentiality and the non-repudiation. It includes the protection of information systems[8] against unauthorized access and actions to corrupt information, as well as the conditions for restoring the functioning of information systems by using their capabilities of protection, detection and rejection.

Although the phenomenon of information vulnerability affects a large number of public or private institutions, with special consequences, it gets dramatic accents when it comes to national defence. It should be added that, in the event of a conflict, the informational elements will be at the centre of a generalized, long and meticulously prepared electronic war.

Access to classified information is permitted in compliance with the principle of the *"need to know"* only to persons holding a security certificate or access authorization valid for the level of classification required to perform the duties of the service. Information that, although not in the scope of classified information, is not intended for the public, constitutes information with limited access.

In the military regulations, information protection for combat actions is included in what is called information operations and includes any activity that prevents the adversary from obtaining, transmitting, processing and using information relevant to the operations of Allied forces.

The protection measures must ensure the continuity of the information services[9], which include: information and communication technology infrastructure, information and electromagnetic spectrum management, communication paths, computing power (computer networks, software and databases), network operations included in the global international network.

These measures shall include at least:

- Operational security (OPSEC);

[7] *Joint Information Operations Planning Handbook*, Joint Forces Staff College, National Defence University, Norfolk, 2002, pp.1-7.

[8] *AJP 3-10*, *op. cit.*, art. 0124.

[9] *Information Operations*, Air Force Doctrine, dc.2-5/2002. p.70.

- Information security (INFOSEC);
- Protection against the enemy's actions regarding the surveillance and recognition of the battle space and the detection of targets.

Particular pressure on the protection of information of a military character, in particular, a media manifesto, whose *"sensational hunger is special"*[10]. Therefore, the protection of state and therefore military secret information and the prevention of their leakage in the public information activity is in the attention of the public and military authorities of all countries and is considered as a condition of ensuring national security, being guarded as the mass media does not present information and data regarding areas that cooperate in the realization of the country's defence strategy, as well as the measures expected to be taken in time of peace or war to counteract an aggression.

CONCLUSIONS

Given that a possible cyber war can only develop on the Internet and implicitly by connecting computers to the electricity grid, we cannot help but dream of a future where, by innovating new security mechanisms that counteract the threats generated by the development of new technologies and media, and think about computer and communications applications, support for command and control of military operations, running based on an operating system proper to the Romanian Armed Forces, thus eliminating all the implications of using the Windows operating system, both on computers independent as well as at network level and, why not, attribute to the communication structures the abilities of an Internet provider for own forces, thus protecting the confidentiality, integrity and availability of information.

BIBLIOGRAPHY

1. ***, *FM 100-6, Information Operation*, 1996.
2. ***, *Joint Information Operations Planning Handbook*, Joint Forces Staff College, National Defence University, Norfolk, 2002.
3. ***, *Law no. 182 on 12.04.2002*, on classified information security, the *Official Gazette* no. 248/2002.
4. Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale militare, servicii și tehnologie*, Editura Universității Naționale de Apărare *"Carol I"*, București, 2010.
5. Gheorghe Ilie, Ion Stoian, Viorel Ciobanu, *Securitatea informațiilo*r, Editura Militară, București, 1996.

[10] Gheorghe Ilie, Ion Stoian, Vasile Ciobanu, *op. cit.*, pp.145-157.

PSYCHOLOGICAL IMPACT OF CYBERTERRORISM

Anca SAVU
PhD Candidate, "Carol I" National Defence University, Bucharest

Florentina-Ștefania NEAGU
PhD Candidate, University of Economic Studies, Bucharest

Any act of terrorism constitutes for the democratic societies a real psychological and emotional aggression, capable of producing fears in the mentality of the population. From a semantic point of view, terrorism achieves its ultimate goal here, by creating a climate of insecurity, fear and terror. The act itself, which may be a conventional terrorist attack or one that takes place in the online environment, is sufficient to profoundly influence professional activities, leisure and travel. Therefore, the profoundly intrusive and violent nature of cyberterrorism can encourage the occurrence of psychiatric disorders or risky behaviour. In order to be able to correctly estimate the impact of cyberterrorism, we must first of all identify the psychological profile of the cyber terrorist. Secondly, cyber terrorism is most often part of conventional terrorism, and therefore has a similar impact.

Keywords: cyber space, cyber terrorism, cyber terrorist, organized crime, psychological impact.

INTRODUCTION

Following the attacks of 11 September 2001, a key element of security policies in the USA as well as in other countries of the world was the strengthening of national security. Several political, military and economic analysts, as well as academics and journalists, have estimated that, after these events, terrorist attacks on computer infrastructure or through them will follow[1].

Any act of terrorism constitutes for the democratic societies a true psychological and emotional aggression, able to determine the change of the perception of the population regarding their physical security or the integrity of the personal data that are found in the online environment.

If in the case of terrorist attacks with explosive devices that cause material damage and loss of human lives, the media and psychological impact is high, being immediately felt by people, in the case of cyber incidents the impact on IT infrastructures is even higher, generating significant remediation costs. At the same time, they also have a psychological impact on people because they no longer consider their personal data or virtual assets safe[2].

First of all, cyber-terrorism has an indirect psychological impact on people, as individuals do not immediately realize that what is happening around them is the result of cyber-attacks or the use of electronic devices. To demonstrate it, we will present some examples of the use of such attacks. In 1999, the Pentagon disclosed that it used a *"special weapon"* that allowed it to disrupt the electricity grid of several cities of the former Yugoslavia[3]. In 2002, President George W. Bush signed a directive *"ordering the US government to prepare national plans for offensive electronic warfare against potential enemies"*[4].

[1] C. Maura, *Le cyber-terrorisme. Le discours des médias américains et ses impacts*, Cités, 2009/3 (no. 39), pp. 81-94, https://www.cairn.info/revue-cites-2009-3-page-81.htm, retrieved on 5 September 2019.
[2] Virtual assets represents intangible assets that can be constituted in alternative investments with specific risks, units of account, virtual currencies etc., http://www.cdep.ro/afaceri_europene/afeur/2019/st_2643.pdf, retrieved on 5 September 2019.
[3] *Truth behind America's Raid on Belgrade*, in The Guardian, 28 November 1999, https://www.theguardian.com/theobserver/1999/nov/28/focus.news1, retrieved on 6 September 2019.
[4] J.P Manach, *Le cyberterrorisme est virtuel*, la cyberguerre en préparation, 2006, http://www.internetactu.net/2006/02/24/le-cyberterrorisme-est-virtuel-la-cyberguerre-en-preparation/, retrieved on 6 September 2019.

In April 2005, the USA established the NATO Strategic Command (StratCom), which became operational since January 2014[5]. This military elite unit not only protects America's vital infrastructure but can attack its enemies as well[6]. In December 2005, the US Air Force added *"domination of cyberspace"* to its mission, and a recently declassified document shows that the goal of Donald Rumsfeld, former Secretary of Defense in the mandates of Presidents Gerald Ford and George W. Bush, had been wanting since 2003 to *"fight the Internet"*, which resembled an *"enemy weapon system"*[7].

MEASURING THE PSYCHOLOGICAL IMPACT OF CYBER-TERRORISM THROUGH THE MASS-MEDIA

The development of the agendas of the press structures is based on the premise that the media has a significant influence on the way in which the public identifies the most important topics, a theoretical assumption consolidated on several empirical studies. In this area, there are two main types of approach, one focusing on the elite and the other being fundamentally pluralistic. The elite approach focuses on institutional political power and decision makers, while the second extends the concept of *"political agenda"* to include such factors as the agenda or media agendas[8]. It will be emphasized that the media acts as the main source of political information of the masses inside the state, but also abroad, and all the more because of the development of satellite television programmes but also of the Internet.

They also serve as a *"main channel"* for communicating public fears and wishes of political elites as well as government actors. The traditional media is a great power operator in the contemporary society, with an unequalled influence on the dissemination of information and news. It acts as an intermediary not only between the population and the government, but also within government bodies.

The relationships between cyber terrorism as part of conventional terrorism and the media are just as complex, ambiguous, maintaining an organic and functional link between them[9]. According to the French psychologist Jossé Évelyne *"without*

[5] NATO StratCom Centre of Excellence, About us, 2019, https://www.stratcomcoe.org/about-us, retrieved on 10 September 2019.
[6] J. Lasker, *US Military's Elite Hacker Crew*, 2005, https://www.wired.com/2005/04/u-s-militarys-elite-hacker-crew/, retrieved on 10 September 2019.
[7] A. Brookes, *US Plans to "Fight the Net" Revealed*, BBC, 2006, http://news.bbc.co.uk/2/hi/americas/4655196.stm, retrieved on 5 September 2019.
[8] C. Maura, *op. cit*, pp. 81-94.
[9] P. Mannoni, C. Bonardi Christine, *Terrorisme et Mass Médias*. Topique Revue, 2003, No. 83, pp. 55-72.

the media, modern terrorism would not survive"[10]. In the information age, in our globalized society, the media offers the necessary space for hackers and terrorists to spread the message and terror through the online environment.

The main role of the media in the event of a cyber-attack is to disseminate the news about the attack, both online and on television stations, presenting what was the damage caused by it and what measures were taken to combat it short-term effects.

THE PSYCHOLOGICAL IMPACT PRODUCED BY TERRORIST PROPAGANDA

Terrorist networks recruits intend not only to produce terrorist attacks but also to use them according to their specialized knowledge, to penetrate computer networks and to virus or encrypt their data, in order to obtain money from them upon providing the unique decryption key. These recruits are also used to disseminate terrorist propaganda in the online environment through social networks or by diverting the websites of private companies or state institutions. An eloquent example of hijacking a website, which also constituted a major cyber-attack, is the August 2012 attack on the Saudi Aramco state-owned company, which led to the shutdown of 30,000 computers. The company's computer network was infected with a virus, in an unprecedented act of sabotage. The attack was claimed by a group called the Justice Cutting Sword, which accuses the Saudi government of crimes and atrocities in several countries. The virus caused data to be erased for three quarters of the company's computers, replacing it with the image of a burned American flag[11].

On 18 January 2016, the Paalga Observatory successively published a photo with Mokhtar Belmokhtar[12], which they described as *"the alleged brain of the attacks in Ouagadougou"*[13]. In the January issue of *Le Pays magazine*, the photographs of all the victims were published, giving the sponsored terrorist organizations an idea of the massacre they produced.

Also, the images were taken in the form of other titles and disseminated through three other online newspapers. The purpose of these disseminations is to

[10] J. Évelyne, *Les médias face au terrorisme et aux populations affectées, l'impossible equation*, 2015, www.resilience-psy.com, retrieved on 10 September 2019.
[11] BBC, *Saudi Aramco Oil Giant Recovers from Virus Attack News Technology*, 27 August 2012, https://www.bbc.com/news/technology-19389401, retrieved on 10 September 2019.
[12] Mokhtar Belmokhtar is an Algerian leader of the Al-Murabitoun group, former military commander of the al-Qaeda group in the Maghreb, https://en.wikipedia.org/wiki/Mokhtar_Belmokhtar, retrieved on 10 September 2019.
[13] Alencontre, *Burkina-Faso. De Sankara à Compaoré et la rivalité entre Daech et l'Aqmi*, 18 January 2016, https://alencontre.org/category/afrique/burkina-faso, retrieved on 10 September 2019.

show the extent of the damage, feeding on the terrorism of terrorists, to convey the idea of a stronger military terrorism than the devoted military forces. Terrorists are portrayed by the three newspapers as *"abnormal beings", "the fools of Allah", "criminal minds who believe neither God nor the Devil"*[14].

Terrorists massacre people through a physical war and the media and social networks amplify the psychological impact of these facts. The horror is dramatized and presented in a compassionate tone, so there is a relation between the journalist writing the news and the emotional man reading[15]. Death is staged, mixing emotions and horror. French historian Jean-Pierre Filiu speaks of *"media terror"* to illustrate the media's voracity for the terrorist act. Searching for shock information often causes them to serve as terrorist propaganda vehicles. The media thus becomes the involuntary accomplices of terrorists whose existence and actions make them known[16].

PSYCHOLOGICAL EFFECTS ON THE TARGETS

Before seeing what the effects on the targets are, it is necessary to identify first what the profile of the cyber terrorist is and what his motivations and targets are. As for the profile and motivations of the cyber terrorist, these can be said to be almost similar to those of the classic terrorist, differing only in the combat environment.

The cyber-terrorist is a person with advanced knowledge in the IT field. The purpose is to reach a goal, such as the one assimilated to the terrorist phenomenon, in which the attacks carried out by them are apparently based on political beliefs or the desire to challenge the legitimacy of the target organizations or governments. Analytically, it is found that the aggressions committed by these groups do not reveal a particular pattern.

From the research carried out so far, it turns out that most terrorists do not suffer from mental illness, but they are rational people, who evaluate very well the costs and implications of the terrorist act, regardless of its nature, finally reaching the conclusion that it is profitable.

Joining a terrorist group gives the newcomer a sense of belonging to a community, the power and identity of a man who has problems of social adaptation and beyond. For the attacker, the benefits are not necessarily material, but they consist of meeting spiritual and social needs.

[14] B. Labasse, P. Savary, Thierry Watine, *Les Cahiers du journalism*, Volume 2, numéro 1, 1er trimestre 2018, Les Presses de l'Universite d'Ottawa.

[15] L.Yaméogo, *Les médias, un allié du terrorisme*, Lassané, 2016, http://cahiersdujournalisme.org/V2N1/CaJ-2.1-R007.html, retrieved on 10 September 2019.

[16] J.P Filiu, *Barbarie jihadiste et terreur médiatique.* Cités, *2015,* pp. 27-38.

Those who become part of a terrorist organization are recruited to meet the needs of the organization. In this sense, the recruiter of the terrorist organization has several criteria and is guided in the recruitment process. They range from age, gender, social environment to different qualities that they seek, to carry out certain missions of a terrorist nature.

The key step in creating the psychological profile of a cyber-terrorist is to identify specific common characteristics that must be investigated. Features include innate aspects, such as openness, awareness, extroversion, agreeableness and neuroticism. Also, personal characteristics and characteristics are shaped by life experiences and events that lead to Machiavellianism, narcissism, psychopathy, sensation seeking maturity, aggression, social skills problems, superficiality, lack of self-esteem and personal integrity. The motivating factors of cybercrime come from hacktivism, monetary gain, espionage, sabotage, political and religious beliefs, curiosity, emotions, increased self-worth and the intention to control and manipulate others.

From a motivational point of view, there are the following psychological types of terrorists, namely[17]:

The revenge seeker – acts under the decisive impulse of the desire for revenge for a previous personal affront. He is willing to pay with life or with freedom.

The common law offender – pursues the satisfaction of the cause through violence, whose interests are often material. This can be achieved either directly, by depriving the victim of the existing assets, or for a longer time, by making claims against the victim's relatives (ransom).

The paid criminal – acts on the indication and with the financial and material support of some terrorist organizations, with the objective of suppressing the life of political or military personalities, who oppose the ideas and interests of the organization. Terrorists in this category are usually professional people, who are proficient in several languages or in different fields, with special physical and mental qualities, which allows them to engage in extremely risky actions.

The mentally ill – acts regardless of the case, situation or consequences. It is strongly radicalized and acts from a malicious and irrational impulse.

The religious fanatic – acts violently, considering that he is led by a divine force to defend the religious ideas and conceptions of which he is adept, the victim being any person or entity that contradicts these ideas. He is led by the religious instinct that blinds him and makes him believe that by his actions he glorifies Allah. Usually such terrorists are formed from childhood, being inspired by violence, hatred

[17] S.A Jalil, *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, Global Information Assurance Certification Paper, https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154, retrieved on 10 September 2019.

of *"unbelievers"* and being raised in the spirit of religious fanaticism.

The national martyr – has as motivation the sacrifice for a great cause and for the national interest. He will pay attention to those personalities who, in his opinion and the organization of which he is a member, constitute a problem in the promotion of their national interests, as well as of the group of which he is a member.

The political protester – has a motivation similar to that of the national martyr, but his interests are political in nature.

From our point of view, the cyber-terrorist is a little different from the classic one, considering that he operates in the online environment. From a psychological perspective, a person is not born a terrorist or cyber-terrorist, but undergoes a set of transformations.

According to Maslow's pyramid, for the terrorist organizations, there are three categories of people that can be transformed into cyber terrorists, namely: people with social needs for inclusion and affirmation, people with security needs, people with basic needs[18].

For people with basic needs, the idea of joining a terrorist organization is very appealing given the fact that it can provide material benefits to both themselves and their family. Frustration is a key element in these people. Part of the behaviour of terrorists is related to frustration about the impossibility of meeting certain personal needs, whether they are psychological or physiological, and this leads to acts of aggression.

Closely related to the non-fulfilment of certain needs is the isolation of the rest of the society. Thus, if a person fails to meet those needs, he or she begins to deny any kind of human behaviour and thus becomes isolated from the rest of society. He thus becomes devoid of empathy for the needs of others and develops a destructive anti-social behaviour towards his fellow men.

Another element in this regard is megalomania syndrome. In this case, the individual has an idealized opinion about himself and has no respect for his fellow men. He can become violent if he comes to the conclusion that society does not respect him, does not respect his beliefs and ideals, thus becoming frustrated that it cannot advance on the steps of Maslow's pyramid. This type of individual needs strong affirmation and feels the need to destroy those who oppose it.

According to a document prepared by the United Nations Office on Drugs and Crime (UNODC), al-Qaeda has been recruiting minors for some time to deal with the lack of human resources. It seems that the organization has focused its attention

[18] European Union Agency for Network and Information Security, *ENISA Overview of Cybersecurity and Related Terminology*, September 2017, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, retrieved on 10 September 2019.

on minors with mental disabilities, low IQ, or who come from broken families or poor social backgrounds. The average age among these minors is 13-16 years[19].

Another category that is of interest to terrorist organizations is represented by women. They are not necessarily used in acts of terrorism, but can be used in the process of recruiting and propaganda on the Internet[20].

Cyber-terrorism is an attractive area for modern terrorists for several reasons: it is much cheaper than the traditional methods of terrorism. The modern terrorist only needs a personal computer and an online connection, they do not have to buy weapons or explosives but they can create and deliver computer viruses through a telephone line, cable or network. It is anonymous, which makes it difficult for security agencies to track or identify the source of the attack.

The variety and number of targets is very high, the cyber-terrorist could target multiple computers and networks at the same time. According to studies, critical infrastructures are vulnerable to terrorist attacks because they are extremely complex, which makes it difficult to eliminate all weaknesses. The attack can be carried out remotely, this is very attractive for cyber-terrorists, because it eliminates the rest of the investment they should have made in the case of a traditional terrorist attack (training camps, investments in weapons, psychological training etc.).

Cyber-terrorism can affect more people than traditional terrorism, thus generating a greater impact on the media.

The target categories affected by cyber-terrorism are: citizens, state institutions, private companies.

Critical infrastructures of a state or financial operations (such as online commerce, currency exchange, payment of bills) are largely affected by the acts of cyber-terrorists, but those who are directly affected will suffer much greater psychological stress, as it is in the case of data theft on the debit card that can leave an individual without all the money in the bank account. We cannot underestimate the impact that cyber-attacks may have on people, because different people react differently to such situations. Some people who are directly affected by cyber-terrorism in cases such as losing vital company information that can be used to threaten the well-being of the organization or data subject can lead to fear and the affected person lives under severe stress. The person involved will suffer emotionally

[19] United Nations Office on Drugs and Crime (UNODC), *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*, 2017, Vienna, https://radical.hypotheses.org/files/2016/04/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf, retrieved on 10 September 2019.

[20] D.E Denning, *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in Arquilla, J. & Ronfeldt, D. (Eds.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Chapter eight, pp. 239-288, Santa Monica, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf, retrieved on 12 September 2019.

and this could affect the state of their mental health. In other cases, misinformation uses websites, e-mail and other electronic means to spread rumours about a particular situation, organization or person, leading to chaos among the general public. People will panic and thus financial operations and normal way of life will be disrupted. Therefore, it is imperative that the general public should be well informed about cyber-terrorism and be able to identify the steps that can be taken to address the concern as best as possible[21].

CHILDREN, A TARGET OF CYBER-TERRORISM?

According to the national laws of several countries in the world, the minor children are protected their dignity, integrity against any violations by other people. For example, the Tunisian legislature has a policy that aims to fight against the exploitation of minors by organized crime and to prevent all forms of ideological indoctrination. Among other phenomena that a child may encounter when surfing the Internet are: incitement to hatred, stimulation to join terrorist networks, propagation of terrorist messages through cyber terrorism and cyber racism, which refers to offending and inciting other people to racism[22]. The fight against both types of involvement is an absolute necessity, which requires vigilance from the competent services in the field.

There are multiple attacks in the cyber space on the dignity and integrity of children. These are threats to their human dignity. These lesions occur in many forms, such as organ trafficking, child trafficking via the Internet, *"cyber-drugs"* and *"cyber-racism"*. Secondly, with regard to trafficking in children through the Internet, national laws prohibit the exploitation of children in different forms of organized crime. But the protection of children in cyber space is not limited to these three phenomena. There are also other phenomena that can pose threats to the dignity and integrity of children.

At present, the Internet is at the base of the risks and dangers to which children become victims. Children who use the Internet can fall prey to paedophiles, terrorists and racist movements. This tool is a means of recruiting terrorists. Terrorist groups and recruiters browse Facebook pages and chat blogs with messages looking for receptive people, especially vulnerable young people, to involve them in a private

[21] S.A Jalil, *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, Global Information Assurance Certification Paper, p. 10, https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154, retrieved on 10 September 2019.

[22] M. Gargouri, *La protection de l'internaute mineur face aux actes de cyber-terrorisme*, Village de la Justice. La Communaute des métiers du droit, https://www.village-justice.com/articles/protection-internaute-mineur-face-aux-actes-cyber-terrorisme,32235.html, retrieved on 10 September 2019.

online group, behind which is a terrorist group. The activists recruited from the online environment by terrorists are mostly minors and young people. Most of the dead or trapped terrorists are young people under the age of 18. Young people today are idealists and believe they have the power to change the world. Terrorists take advantage of this normal stage of their intellectual, psychological and biological development to attract and manipulate these young people insidiously, given the proliferation of cyber-attacks that threaten minors on the Internet.

According to the Tunisian lawyer Mohamed Gargouri, crimes in the field of cyber-terrorism to the detriment of children can take two forms, either by presenting terrorist information, or by electronically recruiting children as terrorist activists. In Arab states especially, a phenomenon that has grown in recent years is cyber activism. Although it is widespread in the world, this subject is marked in the Arab world by repression and anonymity. The repression manifests itself through the censorship used by the authorities and even though the terrorists only intending to go from the challenge on the Internet to the action of concretizing the evil. However, terrorism exists and is real.

Facebook sites and pages are considered by Tunisian law as *"other materials or equipment"* used by an organization or individuals to commit terrorist offenses in cyber-space. It should be emphasized that propaganda and advertising are not just activities closely related to psychological warfare, as there are others such as piracy. Computer hacking is a targeted, efficient and automated attack, sufficiently coordinated to paralyze a child's computer activities on the Internet. Piracy can undermine the child's human dignity by illegally exploiting his photographs or information. Hacker groups have lucrative interests and use technological know-how, by infiltrating social networks and putting their talents in the service of their convictions by organizing computer attacks for the purpose of hacking and hijacking children's personal data. Hackers are motivated by money and are linked to criminal organizations. They are willing to sell their services to the best bidder. Forms of cyber activism include fundraising, mobilization, information exchange, planning, coordination and, above all, recruiting terrorists[23].

CONCLUSIONS

Cyber-terrorism has a direct and indirect impact on people. In the first case people do not immediately realize that what is happening around them is the result of cyber-attacks. In the second case people can get a sense of fear, stress.

[23] G. Yang, *Cyber-activism [draft] [#digitalkeywords]*, June 9, 2014, http://culturedigitally.org/2014/06/cyber-activism-draft-digitalkeywords/, retrieved on 15 September 2019.

The main role of the media in the event of a cyber-attack is to disseminate the news about the attack, both online and on television stations, presenting the damage caused by it and the measures taken to combat its short-term effects.

It also influences the population through the media that broadcasts the news in the stream, and which is often negative, because the negative news brings a high rating to a television station or a large number of hits of a web page.

Cyber- terrorism also has a psychological impact produced by terrorist propaganda. The people recruited by organizations are used to disseminate their propaganda in the online environment through social networks or by diverting the websites of private companies or state institutions. A target category that is increasingly affected is represented by young children, most of whom have access to the Internet and can easily fall prey to malicious people.

It should be emphasized that propaganda and advertising are not just activities closely related to psychological warfare, as there are others such as piracy. Computer hacking is a targeted, efficient and automated attack, sufficiently coordinated to paralyze a child's computer activities on the Internet.

BIBLIOGRAPHY

1. ***, *About us*, NATO StratCom, Centre of Excellence, 2019, https://www.stratcomcoe.org/about-us
2. ***, *Burkina-Faso. De Sankara à Compaoré et la rivalité entre Daech et l'Aqmi*, in À *l'encontre*, 18 January 2016, https://alencontre.org/category/afrique/burkina-faso
3. ***, *ENISA Overview of Cyber Security and Related Terminology*, European Union Agency for Network and Information Security, September 2017, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology
4. *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*, United Nations Office on Drugs and Crime (UNODC), 2017, Vienna, https://radical.hypotheses.org/files/2016/04/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf
5. *Saudi Aramco Oil Giant Recovers from Virus Attack News Technology*, BBC, 27 August 2012, https://www.bbc.com/news/technology-19389401
6. *Truth behind America's Raid on Belgrade*, *The Guardian*, 28 November 1999, https://www.theguardian.com/theobserver/1999/nov/28/focus.news1
7. A. Brookes, *U.S. Plans to "Fight the Net" Revealed*, BBC, 2006, http://news.bbc.co.uk/2/hi/americas/4655196.stm
8. Maura Conway, *Le cyber-terrorisme. Le discours des médias américains et ses impacts*, Cités, 2009/3 (n° 39), https://www.cairn.info/revue-cites-2009-3-page-81.htm

9. D.E. Denning, *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in J. Arquilla, D. Ronfeldt (Eds.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Chapter eight, Santa Monica: RAND Corporation, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf
10. J. Évelyne, *Les médias face au terrorisme et aux populations affectées, l'impossible* équation, 2015, www.resilience-psy.com
11. J.P. Filiu, *Barbarie jihadiste et terreur médiatique*, Cités, 2015.
12. M. Gargouri, *La protection de l'internaute mineur face aux actes de cyber-terrorisme*, Village de la Justice. La Communaute des métiers du droit, https://www.village-justice.com/articles/protection-internaute-mineur-face-aux-actes-cyber-terrorisme,32235.html
13. S.A. Jalil, *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, Global Information Assurance Certification Paper, https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154
14. B. Labasse, P. Savary, Thierry Watine, *Les Cahiers du journalisme*, vol. 2, no. 1, Ist Semester, 2018, Les Presses de l'Université d'Ottawa.
15. J. Lasker, *U.S. Military's Elite Hacker Crew*, 2005, https://www.wired.com/2005/04/u-s-militarys-elite-hacker-crew/
16. J.P. Manach, *Le cyberterrorisme est virtuel*, la cyberguerre en préparation, 2006, http://www.internetactu.net/2006/02/24/le-cyberterrorisme-est-virtuel-la-cyberguerre-en-preparation/
17. P. Mannoni, Christine C. Bonardi, *Terrorisme et Mass Médias*, *Topique Revue*, 2003, no. 83.
18. Lassané Yaméogo, *Les médias, un allié du terrorisme*, 2016, http://cahiersdujournalisme.org/V2N1/CaJ-2.1-R007.html
19. Goubin Yang, *Cyber-activism [draft] [#digitalkeywords]*, 9 June 2014, http://culturedigitally.org/2014/06/cyber-activism-draft-digitalkeywords/

FAKE NEWS IN THE 21ST CENTURY

Antonia Teodora MARIȘ
PhD Candidate, "Carol I" National Defence University, Bucharest

The reality of the current century is shaping new security challenges. Spectacular changes in terms of technological progress, the ubiquity of digital technologies, the digital revolution, the global digital order, the constantly increasing importance of digital platforms, the speed at which information is transmitted, the algorithmization of personal life, the power to direct and change public opinion, are only a few features of the 21st century.

With this evolution, threats, risk factors and current vulnerabilities of each state have reached new states of manifestation. In this context, the fake news phenomenon has the potential to influence the attitude and change the perception of entire audience segments.

A first step in combating this phenomenon is to familiarize the population with this concept that is rapidly becoming a threat. Building a strong security culture and identifying vulnerabilities constitute important steps in establishing a good foundation for a secure environment.

Keywords: fake news, security culture, threat, risk, vulnerability, counter-action.

INTRODUCTION

The last decades of mankind evolution have undergone spectacular changes in technological progress; the age in which we live is paradoxical, tumultuous, a world of informational abundance, subject to continuous change. With this evolution, the threats, risks and vulnerabilities of each state have acquired new registers of understanding and manifestation. These changes in the methods of achieving the goal, specific to the 21st century, make it necessary to consolidate a security culture adapted to the specifics of each state.

The ubiquity of digital technologies, the digital revolution, the global digital order, the growing importance of digital platforms, the speed at which information is transmitted, the algorithmization of personal life, the power to change and direct public opinion, the cultivation and aggravation of disputes are just some of the realities of the current century. They tend to fundamentally change the information and emotional ecosystem of our days. These dominant technologies have the power to dislocate knowledge monopolies, to create an alternative reality, to change pillars of stability, with the ability to spread instantly, on a global scale, without editorial or human filters.

In this context, the fake news phenomenon is a topic of interest through the power and speed at which it can meet strategic objectives and destabilize on a global scale.

FAKE NEWS IN THE 21ST CENTURY

Starting from the realities of the present century, we can also establish the vulnerability-threat relationship within the contemporary conflict. This type of conflict, specific to the 21st century, is an asymmetrical conflict that sums up a unitary whole based on the characteristics of the current century. The strong uncertainty, the unpredictability, the increasing importance of social networks and the media, the rapid evolution of technologies, the strong imprint of the irregular forces, the role of the political factor, the multidimensionality of the conflict space are just some of the features of the contemporary conflict.

The reality of the current century reinforces the need for a security culture adapted to each state. The security culture takes into account the new types of threats; this can be defined as the sum of the beliefs, values, practices

of individuals and states that determine what is considered to be a danger or a situation of insecurity in the broadest sense and what the methods, means, ways of counteracting them are[1].

Before talking about fake news, it is vital to understand the definition of truth. According to Neil de Grasse Tyson, there are at least three types of truth[2]:

- Scientific truth – provable by scientists around the world, accepted based on objective, scientific proof;
- Personal truth/belief/personal opinion – this type of truth is actually opinions formed over time, contextually, or information taken from different people;
- Political truth – information repeated many times or believed and accepted either because the person concerned supports certain political figures, or because it is against the ideas promoted by the opposition.

Organizational truth completes the classification presented above – it includes the set of values, principles, mechanisms based on which an institution/organization operates, regardless of its nature and which are embedded in the organizational culture it develops and are the basis for the organizational image put out for its target audience.

It is very important to start with this classification precisely in order to be able to relate to it in the context of *fake news* specific to the contemporary conflict. It is worth mentioning that the personal truth, the organizational truth and the political truth together represent the way in which people perceive reality, the general truth to which they refer when they analyse any situation, a personal filter through which a new event passes.

People are emotional and often irrational beings, functioning on the basis of a personal reality, personal truths already created. Most times people seek confirmation of their beliefs and opinions when they read a news story. The brain seems to block information we do not agree with, selecting the ones that come in support of an already formed idea, preconceived notion. Confirmation bias is actually this tendency of the human being to look for the evidence, examples and situations that support and confirm personal beliefs[3]. We were not created to perceive reality in all its senses; we have our own film, a personal way of perceiving the reality to which we relate. Moreover, information may or may not reflect reality[4]. Controlling perceptions about information can facilitate the formation

[1] Christopher Daase, *National, Societal and Human Security: on the Transformation of Political Language*, Historical Social Research, 2010, p. 22.
[2] Neil deGrasse Tyson, http://youtu.be/TDoufL_Uf4Q, retrieved on 12.08.2019.
[3] Adams Scott, *Win Bigly – Persuasion in a World Where Facts Don't Matter*, Penguin, New York, 2017, p. 16.
[4] Sorin Topor, *Opinions regarding Informational Evaluation Methods within a Contemporary Informational Operation*, in proceedings, the 8th International Conference *Strategii XXI*, vol 3, *"Carol I"* National Defence University, Bucharest, 2012.

of a favourable reality even if it is based on inaccurate information. In the context of contemporary conflict, fake news is based on vulnerabilities in trying to change behaviours.

The term *fake news* is a type of propaganda that consists of spreading false information through traditional media or through social media. These pieces of news, with an uninterrupted and all-encompassing character, which present a distorted truth, usually aim to influence the masses; the speed at which this news is spread is specific to the 21st century and is due to the technological evolution and the social need to know. Thus, under the motto of informed citizens or the right of the public to know, information whose value of truth is very difficult to prove can be delivered, information which otherwise pleases the public[5].

In record time, the *fake news* headline has morphed from a description of a social media phenomenon into a journalistic cliché, as well as into an accusation thrown by politicians. In mid-2016, Buzzfeed's media editor, Craig Silverman, noticed a stream of fully manufactured news that appeared to come from a single city in Macedonia, Eastern Europe. Investigating the situation, he identified more than 140 websites, all registered in the same city, sites with huge audiences, and obtained through the Facebook platform[6].

Without necessarily having an interest in influencing the US political scene, motivated more by the desire for financial gain through advertising on different social platforms, the administrators of the sites in Veles (Macedonia) made sure that their works of fiction earned maximum popularity. The presidential elections, specifically the Republican candidate Donald Trump, were a hot topic in social media (political topics being of great interest in the 21st century). For this reason, fake articles like *Pope Francis Shocks the World, Supports Trump for Presidency*[7] have been exceptionally successful and have, to a degree, influenced people's perceptions of the Republican candidate.

A classification of *fake news* can be made according to the intention of the one who publishes a certain news item. From this point of view, there are two types of fake news: those deliberately published with the intention of creating an effect and those that, undeliberately, do not contain the complete image, but half-truths or out of context situations[8].

[5] Sorin Topor, Ion Călin, Costinel Nițu, Draga-Nocola Crăciun, *Despre informații și sisteme informaționale militare*, Editura Universității Naționle de Apărare *"Carol I"*, București, 2008, pp.152-153.
[6] ***, *You Can Make This Stuff Up*, https://www.aeaweb.org/research/charts/fake-news-impact-presidential-election-2016, retrieved on 19.08.2019.
[7] Hunt Allcott, Matthew Gentzko, *Social Media and Fake News in the 2016 Election*, https://web.stanford.edu/~gentzkow/research/fakenews.pdf, retrieved on 19.08.2019.
[8] ***, *Fake News: What Is It? And How to Spot It*, https://www.bbc.co.uk/newsround/38906931, retrieved on 14.08.2019.

Fake news does not necessarily mean fully inaccurate news, in complete opposition with reality. Half-truths or distorted perception points of view, seen from other angles, can be presented in order to convince the reader of a certain version of reality. Also, such materials may contain subjective interpretations, may present events/situations without context. The higher the dose of truth, the more it can be perceived by the population as a reality. If disassembled, it tends to diminish the audience's confidence in the respective media sources.

The category of fake news published deliberately with the intention of changing behaviours is the one that should arouse the interest of analysts. Written in order to increase or decrease people's confidence in different institutions, to break up alliances, to damage the image of a public person or simply to induce a state of panic in order to achieve a final goal, they have the power to shape perceptions and to change attitudes. Also, if they reach the audience first, it creates a basis of untruth that can be very difficult to dismantle, precisely because of the aforementioned confirmation error. The reasons for this type of news are different; what they have in common, however, is the desire to change behaviours in order to meet goals.

The power of fake news is owed to the fact that people, in general, tend to distribute news they are comfortable with, which confirm already created perceptions and already existing personal or organizational truths about a particular topic. People voluntarily, unknowingly, distribute fake news and thus take part in the campaign of misleading the population. Thus distributed, the news gains a new power, that of the personal or organizational imprint we give when we decide to distribute information.

Another situation is that, in disagreement with certain news, some people apply the *fake news* label just because they are not willing to accept the presented facts as reality. Some people will apply this label just because they do not share the same opinion.

FAKE NEWS VS. DISINFORMATION

The specific novelty of the 21st century in the propaganda and misinformation process is in fact the speed at which this news is spread and at the same time the importance of our digital behaviour which can be an ideal method to manipulate the opinion of the masses. Digital misinformation has the advantage of accurate persuasion, efficient targeting of the desired audience based on the information that some companies or people have about the population. By knowing certain details about the population, a suitable engagement can be made that delivers the information in the most compatible way, taking into account the vulnerabilities of said audience.

In this context, it is worth mentioning that the reader does not react only to the news itself, but also to the reactions already existing in relation to a certain situation. We can conclude from this reality that sometimes it is sufficient for someone to control the first reactions (reactions that take over the power of personal/organizational truth) to influence the mass reaction, not necessarily having to control the facts.

We live in a century where facts matter less and less; what matters is how they are perceived, how they are reported in the online environment and the attitudes that result from these perceptions. The peculiarities of the present century offer the possibility of expressing personal opinions, which sometimes become more relevant than the facts.

It is not possible to outline a model of the person susceptible to *fake news*, but it is possible to make estimates and to highlight conditions in which *fake news* have a higher chance of achieving the purpose for which it was created. These can be among the most diverse: creating information chaos, polarization, confusion, upsetting, changing leadership in different fields, instigating or fuelling riots etc. Feelings of hatred and insecurity among the population, frustration, uprooting, lack of culture and attachment to society are all factors that increase the susceptibility to the *fake news* phenomenon.

Political instability refers to the political downturn, the growing mistrust of the population in the political class, the incoherence and lack of realism of political programmes and corruption. The lack of a minimum political consensus at leadership level, on fundamental issues, of strategic importance, is the characteristic of an unstable, vulnerable society[9]. Economic instability, fluctuating prices, labour migration outside the borders are possible arguments for economic instability. Regarding the instability on the social level in Romania, it is visibly compounded by social anxiety, the degradation of the perception of national value systems, corruption, tension and distrust in the pillars of society.

The digital platforms and the internet make it possible to present facts instantly. These are many and can meet the most varied expectations, concerns or assumptions. Being confronted with social instability, people tend to extract only the aspects that reinforce their preconceptions and assumptions. This does not mean that the facts are false; they are only presented from a certain angle, a certain point of view, partly true, meant to, in time, shape a certain type of behaviour.

Fake news is very difficult, if not impossible, to differentiate from true information. It is very well camouflaged in current rhetoric and is designed to attract news consumers. Sensational headlines, specially chosen to increase the number

[9] Alina Bârgăoanu, *#FakeNews. Nouna cursă a înarmării*, Editura Evrika, București, 2018, p. 86.

of readers or for the news to be distributed quantitatively in the online environment, are just one of the methods, difficult to refuse, used to gain as many readers or as many hits possible.

It is worth mentioning that, although the information is delivered in the online environment, the emotions unleashed, the feelings created are all of real consequences. Although the information may have been created by false identities/ entities, its effects can influence actual individuals who, under its persuasion, make decisions and resort to actions[10].

A first step towards differentiating between real news and fake news is to strengthen the security culture among the population. The population's security culture concerns the general perceptions of who our enemies are, how they threaten us and how we can act or react effectively. The security culture educates, representing a system of systems, with complex, interdependent functions.

Also, how certain situations/events/facts are described is essential for the group of people to whom they are addressed. The way the article attacks the vulnerabilities of the online news reader actually describes the segment of the population that it wants to influence.

THE FAKE NEWS PHENOMENON – A PHENOMENON WITH POTENTIALLY HUGE SOCIAL IMPACT

Following the 2016 US presidential elections, it was claimed that *fake news* may have played a pivotal role in Donald Trump's victory. On average, one US adult has read and recalled one or more fake news articles during the election period, with a higher exposure to pro-Trump articles than to pro-Clinton articles. How much this has affected the election results depends on the effectiveness of exposure to fake news in changing perceptions regarding voting options.

During this campaign, factually inaccurate information was posted online. It was said that Hillary Clinton was severely ill or that she had sold weapons to the Islamic State terrorist organization[11]. Claims of this sort, popularized by fake news, were adopted by major web sites and national level broadcasters, further fuelling conspiracy theories.

Pizzagate is an example of fake news that has had a direct and powerful impact on reality. This theory went viral during the 2016 US presidential elections, during which time, the personal email address of Hillary Clinton's campaign manager, John Podesta, was hacked and the emails were subsequently published. Proponents

[10] Alina Bârgăoanu, *op. cit.*, pp. 34-50.

[11] See https://www.snopes.com/fact-check/wikileaks-cofirms-hillary-clinton-sold-weapons-to-isis/, retrieved on 10.08.2019.

of the *pizzagate* theory claimed that these emails contained coded messages linking certain US restaurants to Democratic Party officials in connection to a human trafficking and paedophilia network[12]. Members of the far right and other opponents of Hillary Clinton popularized this theory in the online environment. In response, in addition to the numerous online death threats from employers and employees, a North Carolina man opened fire at a Washington pizzeria allegedly involved in the paedophilia network. *Pizzagate* illustrates the strength of fake news and how such news can be used to meet certain goals.

Spenkuch and Toniatti pointed out that exposing voters to an additional TV campaign ad changes voting shares by about 0.02 percentage points[13]. This suggests that if a fake news article were as compelling as a single TV campaign ad, fake news that crowded the internet during the campaign would have had the potential to change the voting action considerably. Of course, there are many reasons why a single fake news story could have been more effective than a television commercial. If it were true that the Pope supported Donald Trump, according to the content of one of the fake news articles, this would be significantly more surprising – and would probably move the beliefs of a rational voter more than the results of information in a typical campaign ad, garnering more support.

To the extent that fake news imposes social costs, what can and should be done? In theory, one should want to address the failures that lead to distortions, which would take the form of increasing information about the state of the world and increasing the incentives for news consumers to deduce the true state of the world. In practice, social media platforms and advertising networks have faced some pressure from consumers and civil society to reduce the prevalence of fake news on their platforms. For example, both Facebook and Google remove fake news sites from their advertising platforms because they violate policies against misleading content[14].

Moreover, Facebook has taken steps to identify fake articles, to mark them as *"third party disputed"*, reducing their inclusion in user news feeds and helping users avoid accidental sharing of fake articles by notifying that the story is *"challenged by third parties"* before sharing it[15]. These actions have the potential to have a positive social impact, but identifying fake news sites and articles also raises important

[12] See http://www.cuvantul-ortodox.ro/recomandari/sensul-razboiului-impotriva-stirilor-false-nu-filtrarea-critica-a-stirilor-ci-monopolul-asupra-viziunii-corecte-despre-lume-este-cruciada-impotriva-fake-news-menita-acoperirii-scandalului-pizza/, retrieved on 19.08.2019.

[13] Jörg L.Spenkuch, David Toniatti, *Political Advertising and Election Outcomes,* CESifo Working Paper Series 2016, pp. 23-24.

[14] Nick Wingfield, Mike Isaac, Katie Benner, *Google and Facebook Take Aim at Fake News Sites*, New York Times, 2016, pp. 32-35.

[15] Hunt Allcott, Matthew Gentzkow, *op. cit.*, p. 14.

Wquestions about who becomes the arbiter of truth.

During the latest presidential elections in the United States of America, it is appreciated that online social media platforms have played a defining role in the outcome and *fake news* played a central role. It is estimated that, at this poll, the 20 most known fake news generated 8.7 million actions, reactions and comments on the online social platforms, compared to the only 7.4 million reactions and comments generated by the 20 most known real news on the most reputable news web-sites[16]. Mark Zuckerberg himself has publicly stated that approximately 126 million Americans viewed on Facebook social media platform fake political news during the 2016 presidential elections in the United States of America. There is no data on the percentage of people who accessed the pieces news or were influenced by them, but the situation may raise a series of hypothetical discussions about manipulating the intention to vote, affecting the confidence of the electorate in elections[17]. At the same time, Mark Zuckerberg, has said on his personal Facebook account that he is trying to *"reduce misinformation, block spam messages from which certain authors benefit, or only seek more visits to their own sites"*.

In the article *A New Educational Tool against Misinformation*, published in the Facebook Newsroom section, Adam Mosseri, production manager at Facebook, said that the platform tried to stop the spread of false information as much as possible and focused on three major directions: disrupting economic incentives (because most often promoters of fake news are financially motivated), building new products and providing support to users in making decisions when faced with such situations[18].

The *fake news* phenomenon has the potential to distort election campaigns, affect public perception or influence human emotions, these effects being speculated by people who generate virtual robots that can even engage in more complex types of interactions, commenting on people's posts and answering questions, thus manipulating real users and affecting their perception of reality[19].

[16] Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook*, https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-newsoutperformed-real-news-on-facebook, retrieved on 19.08.2019.

[17] Carol E. Lee, Jo Ling Kent, *Facebook Says Russian-Backed Election Content Reached 126 Million Americans*, https://www.nbcnews.com/news/us-news/russian-backed-election-content-reached-126-million-americans-facebooksays-n815791, retrieved on 19.08.2019.

[18] Andrei Elena Adelina, *Facebook vs. Fake News*, https://intelligence.sri.ro/facebook-vs-fake-news/, retrieved on 19.08.2019.

[19] Ferrara Emilio, Onur Varol, Davis Clayton, Menczer Filippo, Flammini Alessandro, *The Rise of Social Bots. Communications of the ACM*, Vol. 59, No. 7, 2016, pp. 96-104.

FAKE NEWS – THREAT TO NATIONAL SECURITY

Considering what type of attitudes it can lead to, in what way fake news can influence, it must be taken into account that this phenomenon can pose a threat to the security of any state. The strategic objectives of the different regional powers can be achieved using this tool. Using the internet and social media, a news story can influence a very large number of people in a very short time.

Several states have begun to understand the impact and power that this phenomenon can have and have started to take measures in this regard, especially after the scandal caused by the accusation of using fake news as a tool to manipulate the population during the 2016 US presidential elections.

Due to the impact they may have on the population or even the decision-makers of a state, fake news in this category may represent threats to national security. In such a context, which is no longer related to guaranteeing freedom of expression, but to preventing the misuse of the media (both traditional and digital), combating fake news becomes a legitimate concern that should draw the attention of decision-makers of every state.

It is worth mentioning the fact that the phenomenon has the potential to influence the opinion of the masses, as well as the opinion of key decision-makers.

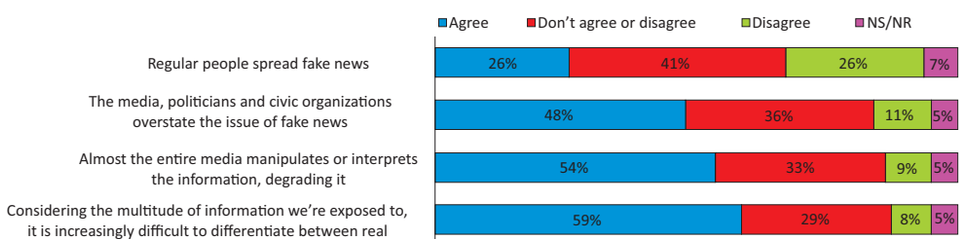


Figure no. 1. Poll results – Romanians' perception of fake news[20]

The sociological study conducted by the International Political Science and International Relations Institute *"Ion I. C. Brătianu"*, part of the Romanian Academy, in collaboration with the Information War Analysis and Strategic Communications Laboratory (LARICS), asked respondents to place each statement from the 4 existing ones in one of these categories: I agree, I don't agree or disagree, I disagree, I don't know/I won't answer (NS/NR).

[20] Matei Alexandru, *SONDAJ Peste jumătate dintre români cred că politicienii sunt principalii autori și propagatori de fake news,* https://www.g4media.ro/sondaj-peste-jumatate-dintre-romani-cred-ca-politicienii-sunt-principalii-autori-si-propagatori-de-fake-news.html, retrieved on 19.08.2019.

The results of the study show the following[21]:

- More than half of Romanians consider that behind the spread of fake news are, most of the times, politicians and parties in their country; they, the politicians, are considered to be able to use any means to achieve certain strategic objectives;
- The majority of respondents from Romania (56%) consider fake news as being more spread out through the online environment, compared to traditional channels;
- The majority of respondents from Romania (54%) are aware that most of the media adds a personal touch and interpretation to the information that is being disseminated;
- 59% of respondents are aware it is difficult to differentiate between fake news and real news;
- A small margin of respondents perceive regular people as propagators of fake news.

The survey in Romania was conducted by *Inscop Research* (www.inscop.ro) between 12 and 23 October 2018, on a sample of 1050 subjects, representative for the population of Romania, noninstitutionalized, aged 18 years and above. The maximum permissible error of the data is ± 3%, at a 95% confidence level on a multi-layered, probabilistic sample type. The method of collecting the data was that of the opinion poll based on a questionnaire applied by the interview operators at the respondents' home. The sample was validated on the basis of official data of the National Institute of Statistics[22].

The report *Security Culture and the Fake News Phenomenon*, based on the results of an opinion poll conducted between November 2018-January 2019, aimed to identify perceptions regarding the culture of security and fake news. The questionnaire included 25 questions to which 293 respondents answered. The no. 17 question of the above report is the following: *Who should, in your opinion, deal with identifying and combating fake news?* I chose to highlight the results of this question from the questionnaire in order to highlight how the population assigns responsibility for identifying and combating this phenomenon.

The results of the report highlight the following aspects:

- Individual responsibility is essential in identifying and combating fake news – each news consumer, individually, must make the effort to identify and report these news: 75.7% of responses;
- Institutional responsibility is also important, the respondents appreciating the role of a state institution with this type of task (53.1%) regarding the fight against the *fake news* phenomenon.

[21] *Ibidem.*
[22] *Ibidem.*

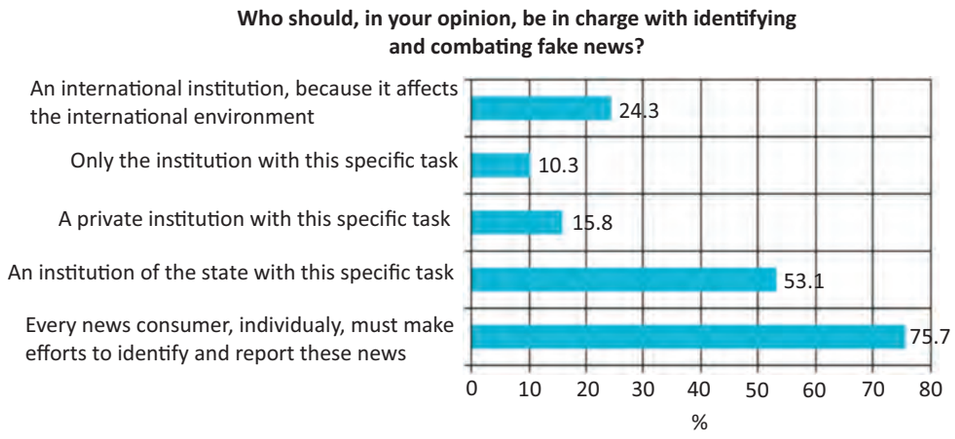


Figure no. 2. Survey poll – who is responsible with identifying and combating fake news[23]

CONCLUSIONS

Digital media is threatened by the danger that real news will be impossible to differentiate from fake news. A real problem is the lack of an adequate legislative framework. At this time, in Romania, there are several legal provisions that refer to, generically, the obligation of the press to transmit truthful information, without however being able to be applied exhaustively, regardless of the propagation environment, including at the level of some forums, comment sections or social media platforms[24].

At this time, it is very difficult to draw a clear line between an effective legislative measure and the need to respect the freedom of expression, the foundation of any democratic society. The scope of the fake news phenomenon and the possible consequences of this type of influence entail the need to adopt a legislative framework dedicated to the clear definition of the phenomenon, sanctions and measures to be taken.

It is very difficult to know exactly whether the pieces of news we are reading are real or not. But, based on some principles to guide our behaviour, we have a higher chance of not being misled by fake news. Considering this, I suggest the following:

- Regarding the attitude of each individual and improving the awareness of the risks we are exposed to, I suggest the following measures:
- Training critical thinking;

[23] Ruxandra Buluc, Ioan Deac, Răzvan Grigoraș, Ciprian Lungu, https://www.proscop.org.ro/site/wp-content/uploads/2019/09/raport-cutura-securitate-fake-news.2.pdf, p. 121, retrieved on 17.09.2019.
[24] Andrei Elena Adelina, *op.cit.*, p. 45.

- Assessing the credibility level of the news agency that published/ distributed the news;
- Verifying information from multiple unrelated sources before taking it as truth;
- Verifying the date on which the article was published, in order to have an understanding of the timeline;
- Reading the entire article, in order to have a good understanding of what is being stated. Often, articles have a catchy title that is almost unrelated to the actual content they present;
- Awareness of one's own confirmation bias in order to see if the power and impact a certain piece of news has on a person is actually related to the power of confirming personal beliefs;
- Making sure the article is not satirical in nature (parody).

Regarding the attitude of each person and improving the awareness of the risks we are exposed to in the online environment, I suggest the following measures:

- Cultivating a security culture adapted to current realities and implemented among the population;
- Awareness programmes for individuals/institutions of strategic importance, likely to be targeted by hostile entities;
- Media literacy (establishing an agreement between title and text, checking authors and sources, consulting anti-fake news web-sites);
- Digital literacy;
- Controlling explicit digital behaviour (better knowledge of the consequences that our actions can have in the online environment);
- Increasing the resilience of the population to fake news by raising awareness of the possible risks and threats in the online environment;
- Rating sites according to the production of fake news (black lists containing the sites that are responsible for promoting fake news; establishing a credibility ranking for each site);
- Cutting advertisement income for the accounts and web-sites that distort information;
- Adopting a clear and transparent policy regarding virtual identities and bots, taking measures to close/ban fake accounts;
- Identifying vulnerabilities in perception and attitude of the population.

It is imperative that we should be aware of what we read, believe, distribute. The naive digital behaviour of the online media consumer can have a negative impact on our future.

BIBLIOGRAPHY

1. Scott Adams, *Win Bigly- Persuasion in a World Where Facts Don't Matter*, Penguin, New York, 2017.
2. Alina Bârgăoanu, *#Fake news, Noua cursă a* înarmării, Evrika Publishing, București, 2018.
3. Christopher Daase, *National, Societal and Human Security: on the Transformation of Political Language*, Historical Social Research, 2010.
4. Joseph Dominick, *Ipostaze ale comunicării de masă. Media în era digitală*, Comunicare. ro, București, 2009.
5. Emilio Ferrara, Varol Onur, Davis Clayton, Filippo Menczer, Alessandro Flammini, *The Rise of Social Bots. Communications of the ACM* ,Vol. 59, No. 7, 2016.
6. B.J. Fogg, *Persuasive Technology: Using Computers to Change What we Think and Do,* Burlington, 2003
7. Richard Flecher, Alessio Cornia, Lucas Graves, Rasmus N. Kleis, *Measuring the Reach of Fake News and Online Disinformation in Europe,* FACTSHEET, 2018.
8. Andrew Keen*, Hot to Fix the Future. Staying Human in the Digital Area*, St. Martin's Press, London, 2018.
9. Jörg Spenkuch, David Toniatti, *Political Advertising and Election Outcomes*, CESifo Working Paper Series, 2016.
10. Sorin Topor, *Opinions regarding Informational Evaluation Methods within a Contemporary Informational Operation*, proceedings, the 8th International Conference *Strategii XXI*, Vol. 3, Editura Universității Naționale de Apărare *"Carol I"*, București, 2012.
11. Sorin Topor, Ion Călin, Costinel Nițu, Draga-Nocola Crăciun, *Despre informații și sisteme informaționale militare*, Editura Universității Naționale de Apărare *"Carol I"*, București, 2008;
12. Marian Voicu, *Matrioșka mincinoșilor. Fake news, manipulare, populism*, Editura Humanitas, București, 2018.
13. Nick Wingfield, Mike Isaac, Katie Benner, *Google and Facebook Take Aim at Fake News Sites*, New York Times, 2016.

WEBOGRAPHY

1. https://www.proscop.org.ro;
2. https://ec.europa.eu;
3. https://intelligence.sri.ro;
4. https://web.stanford.edu;
5. https://www.aeaweb.org;
6. https://www.bbc.co.uk;
7. https://www.buzzfeednews.com;
8. https://www.g4media.ro;
9. https://www.nbcnews.com;
10. https://www.snopes.com/;
11. http://www.cuvantul-ortodox.ro.

FAKE NEWS – THREAT TO NATIONAL SECURITY AND DEFENCE –

Sorina Ana MANEA

PhD Candidate, "Carol I" National Defence University, Bucharest

In the last four years, fake news has overtaken the cancan and the mundane world to be used as a "weapon" in the arsenal of social manipulation.

Fake news is today a very effective tool by which democratic institutions are eroded and the state entities demonized.

Although most often the identity of the perpetrator, of the one who triggers a fake news directly or through a software application, is unknown, the state must fulfil its obligation to maintain national security and to ensure the nation's defence, as well as to guarantee the exercise of the fundamental rights and freedoms of man and, increasingly, the obligation to guarantee the right of citizens to be properly and truthfully informed.

The eradication of the fourth power, by shifting information from professionalism to the "tweet" news, makes these state obligations much more difficult to fulfil.

This article brings to the readers' attention a series of effects generated by fake news and how they have or can have an impact on national security and national defence.

Keywords: fake news, democracy, propaganda, subversion, security and national defence.

PRELIMINARY REMARKS

"False (fake) news is a type of yellow journalism[1] or propaganda, which consists of spreading false information through traditional media or traditional social media, such as TV or newspapers. Fake news is written and published with the intention of misleading, in order to damage the reputation of an agency, entity or person, as well as for financial or political gain, often using sensational, dishonest, or simply manufactured headlines to increase the number of readers, for the spread in the online environment and for revenue through clicks on the Internet. In the latter case, it is similar to sensational clickbait[2] titles from the online environment and is based on the revenue generated, regardless of the truthfulness of the published stories. False news intentionally misinforms and differs from satire or parody, which are intended to amuse the public, rather than mislead it.

The relevance of fake news has grown in the post-truth political system. For the media, the ability to attract readers to their sites is required to generate revenue from online advertising. If publishing fake content attracts users, it benefits advertisers and improves their opinions. Access to online advertising revenue, increasing political polarization, and the popularity of social media platforms, such as Facebook, have all been involved in spreading fake news, competing with legitimate news. Political or government actors have also been involved in generating and disseminating fake news, especially during election"[3].

I chose to cite the definition of fake news offered by Wikipedia precisely because this site has become the first choice as a source for primary information for any Internet user, and I make a reasonable assumption by saying that it is the first site accessed to find out more about any aspect that interests somebody,

[1] *Yellow journalism or the yellow press* is a model of journalism, which presents small or poorly documented news and relies on attractive headlines to sell more newspapers. The techniques may include exaggerations of events, scandals and sensationalism, https://ro.wikipedia.org/wiki/Jurnalismul_galben, retrieved on 12.09.2019.

[2] *Clickbait* is a form of fake advertising that uses hyperlink text or a thumbnail link, designed to attract attention and entice users to watch that link, read, view or listen to the piece of content online, with a defining feature of being deceptive, usually sensationalized or confusing, en.wikipedia.org/wiki/Clickbait#cite_note-2, retrieved on 12.09.2019.

[3] See https://ro.wikipedia.org/wiki/%C8%98tiri_false#cite_note-wired.com-1, retrieved on 15.09.2019.

considering that, in August 2018, it recorded 20 billion views, and between August 2017 - August 2018, had a total of about 500 billion views[4].

Particular to Wikipedia is also the fact that anyone can contribute with articles, whose accuracy depends on the edits that other users are making based on the approval obtained from the administrators, and on the presumptions of their ethical behaviour and the fact that manipulation through such platforms is more difficult[5].

The *fake news* phenomenon has grown especially in the last four years, as a result of the public awareness formed based on the impact it had on the 2016 US presidential elections. However, this phenomenon has not manifested, and is not manifesting itself only in the United States of America, being spread all over the world, as a consequence of globalization and of the negative effect of the generalist interpretation of freedom of expression.

In 1947, Gordon W. Allport and Leo Postman, defined the rumour as *"specific (or topical) proposition for belief, passed along from person to person, usually by word of mouth, without any secure standards of evidence being presented. The implication in any rumour is always that some truth is being communicated. This implication holds even though the teller prefaces tidbit with the warning, <It's only a rumour, but I heard> ..."*[6].

The rumour is for Knapp (1944) *"a proposition for belief of topical reference disseminated without official verification"*[7].

Tamotsu Shibutani (1966) defined rumour as *"a recurrent form of communication through which men caught together in an ambiguous situation attempt to construct a meaningful interpretation of it by pooling their intellectual resources"*[8].

Jean-Noel Kapferer defined rumour as *"the emergence and circulation within the society of information either still not publicly confirmed by official sources or denied by them"*[9].

[4] See https://stats.wikimedia.org/v2/#/all-projects/reading/total-page-views/normal|bar|2-year|~total|monthly, retrieved on 13.09.2019.

[5] Sanmay Das, Allen Lavoie, Malik Magdon-Ismail , *Manipulation among the Arbiters of Collective Intelligence: How Wikipedia Administrators Mold Public Opinion*, https://www.cse.wustl.edu/~sanmay/papers/wiki-cikm.pdf, retrieved on 13. 09.2019.

[6] G. W. Allport, Leo Postman, *The Psychology of Rumor*, Henry Holt and Co., New York. 1947, p. IX.

[7] Robert H. Knapp, *A Psychology of Rumor*, The Public Opinion Quarterly Vol. 8, No. 1 (Spring, 1944), Oxford University Press on behalf of the American Association for Public Opinion Research, p. 22.

[8] Tamotsu Shibutani, *Improvised News: A Sociological Study of Rumor, University of Santa Barbara*, Bobbs – Merill Company Inc. 1966, p. 17, https://archive.org/details/improvisednewsso0000shib, retrieved on 13.09.2019.

[9] Jean-Noel Kapferer, *Managing Brands through Rumors*, in W. Wunderlich, M. Bruhn eds (2004) Medium Gerücht, Haupt Verlag, https://www.researchgate.net/publication/278812817_Managing_brands_through_rumors, retrieved on 13.09.2019.

Nicholas DiFonzo and Prashant Bordia believe that *"Rumour is similar to news in this way; it tends to be information that is new."*[10]; *"is intended as a hypothesis to help make sense of an unclear situation whereas gossip entertains, bonds, and normatively influences group members"*[11].

Why is rumour relevant when discussing fake news? Because rumour has been a social manipulation mechanism, at least in the last hundred years, that has had results, mostly after the consolidation of the traditional modern press. However, nowadays, rumour has become a refined art form of manipulation and this even if *"the use of propaganda is old, but so far technology has not been so effective in disseminating it"*[12]. In Romania, relevant to this phenomenon has become the expression *"sources say..."*.

THE STATE, THE PRESS AND THE RIGHT TO INFORMATION

According to the principles of democracy, every individual has the right to be accurately informed. This right, fundamental in any democratic society, has been increasingly assaulted over the last 20 years, and the negative impact is huge.

The Internet has facilitated globalization, initially understood as a form of integration of national economies into a global market economy. However, with the emergence and development of social online networks, globalization extends to the individual, that is, in addition to forming a virtual alter ego, the individual's opinion has become a focal point, one of polarization and amplification of a message, while maintaining anonymity and blurring to extinction the need for truth, for the real of those transmitted. In other words, Facebook, and especially Twitter, have metamorphosed some traditional users, presumed as individuals, but sometimes only applications, in the bearer and spokesman of a virtual message from point A to all the actual, physical, points by means of a simple click – communication many-to-many[13].

In 2005, journalist Thomas Friedman wrote about globalization in the following terms: *"Globalization 1.0 (1492 to 1800) shrank the world from a size large to a size medium, and the dynamic force in that era was countries globalizing for resources*

[10] Nicholas DiFonzo, Prashant Bordia, *Rumor Psychology: Social and Organizational Approaches*, 1st ed., Hamilton Printing, Castleton, 2007, p. 16.

[11] *Ibidem*, p. 23.

[12] N. Nougayrede, *In this Age of Propaganda, We Must Defend Ourselves*, The Guardian 31.01.2018, https://www.theguardian.com/commentisfree/2018/jan/31/propaganda-defend-russia-technology, retrieved on 14.09.2019.

[13] Damien Smith Pfister, *Networked Expertise in the Era of Many-to-Many Communication: On Wikipedia and Invention*, Social Epistemology, Papers in Communication Studies. 10 July 2011, pp. 217–231.

and imperial conquest. Globalization 2.0 (1800 to 2000) shrank the world from a medium size to a size small, and it was spearheaded by companies globalizing for markets and labor. Globalization 3.0 (which started around 2000) is shrinking the world from a small size to a tiny size and flattening the playing field at the same time. And while the dynamic force in Globalization 1.0 was countries globalizing and the dynamic force in Globalization 2.0 was companies globalizing, the dynamic force in Globalization 3.0 – the thing that gives it its unique character – is individuals and small groups globalizing. Individuals must, and can, now ask: where do I fit into the global competition and opportunities of the day, and how can I, on my own, collaborate with others globally? But Globalization 3.0 not only differs from the previous eras in how it is shrinking and flattening the world and in how it is empowering individuals. It is also different in that Globalization 1.0 and 2.0 were driven primarily by European and American companies and countries. But going forward, this will be less and less true. Globalization 3.0 is not only going to be driven more by individuals but also by a much more diverse – non-Western, non-white – group of individuals. In Globalization 3.0, you are going to see every color of the human rainbow"[14].

Another feature of Globalization 3.0 is that it does not exclude the other two types of globalization, but overlaps them, amplifying them and, at least from the perspective of Globalization 2.0, drawing resources from it, through the social media and high-tech giants. The Internet and Globalization 3.0 erode the patterns of the social mind and rewrite the way we live. The dynamism of social, economic and political changes takes place against the backdrop of states' resistance to change. States, as primordial bureaucratic entities, do not have the flexibility to cope with the alert pace of visualized society. Being of a Hobbesian source, a consequence of Globalization 1.0 and 2.0, the state must ensure the needs of the society it represents and must ensure the fulfilment of its positive and negative obligations, even in the context in which social and, above all, individual life, are rapidly gaining a new dimension – the virtual one.

The phenomenon of rule erosion, and of authority in general, caused by the Internet and globalization, has increased through the development of social media, a good example for this being the difficulty with which the state intervenes to protect the right to information of citizens, especially in the context the rapid disappearance of the traditional press.

[14] Thomas L. Friedman, *It's Flat World, After All*, The New York Times Magazine, Section 6, April 2005, p. 3.

In Romania, in the summer of 2018, on the website of the Union of Professional Journalists from Romania, a call was posted regarding the disappearance of the traditional media, signalling among others that: *"In what way and how much longer can the written press last?"* First of all, it is feasible to analyse the phenomenon in order to discern a rule, a tendency in media developments under the impact of IT. Attempts, a bit shy yet, exist. For example, the Union of Professional Journalists in Romania launched at the beginning of 2017 on the first page of its own site an opinion poll, addressed mainly to journalists, in which a first question was: *"Do you think the print media will be able to recover the lost ground to online information sources?"*. Only 25 percent of the answers were YES, and 72 percent were pessimistic – NO. The sample of respondents was not very large, but I also think that the conclusions are not far from the truth.

"Tabloidization, on the other hand, in the audio-visual media and in the media offered by the Internet – such as the websites, or the colourful little ones offered in plenty at the kiosks – have a common purpose, namely to attract as much advertising as possible. And the money in the advertising comes mainly to those <publications> that prove they have traffic, so unique readers. As in war or in love, in battles carried out for the purpose of attracting readers all means are allowed, we find exaggerated headlines for two-cents news in order to entice readers to <click>, <admire> as far-flung, vulgar photos as possible and we are tempted with promotions of all kinds. And much of the information provided with tam-tam is proven to spring from the imagination and speculation of those who produce it. You can find everything out there except honesty and respect for those to whom it is addressed"[15].

The effects of the disappearance of traditional, printed media are discussed by Director of Centre for the Study of Media, Communication and Power and Senior Lecturer at King's College London, who stated: *"On the night of 13 June 2017, as flames engulfed Grenfell Tower in west London, Rania Ibrahim filmed the scene outside her flat on the twenty-third floor of the tower […] During the night, news of the fire travelled quickly across social media. As it spread, offers of help came flooding in: volunteers, donations in kind […]. For days and weeks after 14 June, the terrible fire at Grenfell Tower dominated UK national media and almost toppled the recently elected prime minister, Theresa May. […] Yet their anger was directed almost as much at the media as at the government. <You didn't come here when people were telling you that the building was unsafe>, one man said to veteran*

[15] Corneliu Cârlan*, Presa scrisă moare!,* 14 June 2018, https://uzp.org.ro/3312/presa-scrisa-moare/, retrieved on 15.09.2019.

Channel 4 presenter Jon Snow when he visited the burnt-out building. <That is not newsworthy. You come here when people die. Why?> Another held up a sign reading <This is not a photo opportunity> and shouted <This is real life!> […] There was no coverage because there were no longer any journalists dedicated to reporting on Kensington and Chelsea"[16].

Martin Moore believes that the disappearance of the printed media is only a symptom of the profound changes that the globalized society is experiencing, and these changes are visible in the conflict between private and public, between libertarianism and authority, conflict affecting the election system and democracy.

"Democratic elections and political events all over the world were becoming synonymous with pitched battles between partisan groups, cyber-muggings and flame wars. Political campaigning online, in other words, was looking less like democratic deliberation and more like information warfare.

This deliberate transgression and destruction of democratic norms in the digital sphere has been driven forward by those who prize freedom and sovereignty online above all else. For this reason, you might call these people free extremists, or freextremists for short. Yet freedom, even in the most libertarian societies, has never been absolute. Nowhere is it legitimate, for example, to harm others in the pursuit of freedom – except in the context of war. This is presumably why many freextremists justify their behaviour by claiming they are in a virtual conflict with those who have different values than they do and who seek to inhibit their freedoms. Yet the consequence of this is an uninhibited, aggressive, violent and hyper-partisan online space, where democratic processes of debate, respect, civility and compromise are collateral damage"[17].

The state must face the *"war"* between the public and the private, promoted in the virtual environment and based on an ultra-libertarian ideology that can be found in the politics of the web giants. This ideology is based on ideas that have origins in 4chan type demonization campaigns, as well as the tactics of tailored messages practiced by Cambridge Analytica type of companies. Such campaigns have shown the world how easily the public, the electorate, but also the electoral system of any nation can be manipulated.

"The revolution in digital communications – the collapse of news media and the rise of dominant tech platforms like Google, Facebook and Twitter – is buffeting

[16] Martin Moore, *Democracy Hacked. Political Turmoil and Information Warfare in the Digital Age*, A Oneworld Book, 2018, pp. 166-168.
[17] *Ibidem*, pp.35-36.

our elections, capsizing conventional candidates and drowning centrist parties. More than that, it is restructuring our politics, undermining existing institutions and remaking the role of the citizen. It is creating openings for those who previously had none, space in which to sidestep norms, rules and established practices, and opportunities for gaming and distortion. If we are to have any chance of determining the type of political system that will emerge from this maelstrom, then we need to start by trying to understand it"[18].

The destabilization of the electoral system undoubtedly leads to the destabilization of the democratic state, the scaffolding of this kind of social organization, and the erosion of national values established through the agreement of the society. The corruption of the electoral system delegitimizes the constitution of the representative bodies of the democratic society and thus the fundamental rights and freedoms are affected, from the perspective of social constructions, as well as the life of the citizens in the most real way possible. The corruption of the electoral system can transform a democratic society into a totalitarian one, in which the will of the minority or, worse, of a group, dictates.

The present states are the result of a secular historical process in whose construction time plays an essential role, since it allows the citizens to adapt to the behavioural requirements necessary for the healthy development of the society. But nowadays, time is condensed, and citizens no longer have the attention span stable enough to internalize and understand the rules of the majority. Today everything has to be obtained with a click.

In 2017, the US Senate launched an investigation into the alleged interference of the Russian Federation in the US election process during the election of the president in 2016. During the proceedings, members of the legal committee tried to understand, by hearing the Facebook, Google and Twitter management, how it was possible for Russian commercial entities to purchase targeted ads for US voters in the context in which the two corporations have the largest and most developed big data processing capacity.

The cause of the inability of Internet giants to identify subversive involvement of a rival state or entities is precisely how the Internet is conceived, as a space free from the interference of authority and in which content the information can flow freely. None of the three follows the way in which the advertising space they sell

[18] *Ibidem*, p. xi.

is used, although from 2016 it is obvious that this is the medium of spreading fake news and misinformation, along with posts of individuals or bots[19].

The formation of the Judiciary Committee of the US Senate represents the certification that fake news is no longer just the malicious rumour, but an effective tool to abuse the values of a society.

FAKE NEWS AS A THREAT TO NATIONAL SECURITY

In Romania, fake news campaigns and demonization of leaders, regardless of their political colour, but especially of demonizing public authority, have taken on an unprecedented extent. An example in this regard is the well-known case of the disappearance of a young woman from Caracal, in the summer of 2019, in which the *"news on sources"* are run dizzily, in assumptions and value judgments, which divert public attention from the drama of a young woman to the state, described as an entity separate from its citizens, in whose existence the citizen has no responsibility.

According to a survey conducted by the European Commission *"both Romanians and citizens of the European Union believe that news and information that distort or even falsify reality are often encountered and are even a national problem, mentioned by about seven out of ten people (often encountered – RO: 72%; EU28: 68%; this is a problem – RO: 69%; EU28: 70%). Even if this kind of news and information is easily identifiable in the respondents' acceptance (RO: 59%; EU28: 58%), Romanians believe that the existence of news or information that misrepresents reality or is even false is a problem for democracy overall, with a weight of 7pp lower than the average registered at EU level (RO: 69%; EU28: 76%). Compared to previous years, social networks have been mentioned more and more as sources of information. These are considered by more than half of Romanians (60%, + 7pp compared to 2017) as a modern way of being aware of political issues, but also as a way of expressing their own opinions on these issues, 60% (+ 9pp compared to 2017) among the respondents use social networks for this purpose. At the same time, 58% of Romanians consider that information about political issues on social online networks cannot be trusted, but the latter can arouse people's interest in political affairs, an idea confirmed by 59% of Romanians (+ 9pp compared to 2017)"*[20].

[19] An Internet bot, also known as a web robot, robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone, https://en.wikipedia.org/wiki/Internet_bot, retrieved on 13.09.2019.

[20] *Eurobarometru Standard 90 Raport național, Opinia Publică în Uniunea Europeană*, autumn 2018 http://ec.europa.eu/commfrontoffice/publicopinion p.11, retrieved on 10 September 2019.

In Romania, there are legal provisions that regulate the obligation of the press to transmit objective information, but in the virtual environment, at the level of forums, comment sections or social platforms, where the opinion of the individual becomes news by share, the obligation is only of a moral nature, and the enforcement the provisions of the Criminal Code regarding the communication of false information[21] is difficult[22], if not impossible, if the location of the perpetrator is taken into account.

The communication of false information consists of the action of communicating or spreading by any means, news, data or false information or falsified documents, knowing their false character, if by this the national security is endangered. Although the society recognizes the social danger of such acts, the fulfilment of the condition of knowledge by the perpetrator of the false character of the information he has communicated or spread makes this crime in the online environment a *probatio diabolica* situation.

Also, in the happy situation in which the perpetrator is identified *"the action of communicating or spreading the news, data, information or documents becomes criminal only if the perpetrator knows, at the time of the act, their lack reality. It follows, therefore, that doubt about the veracity of the information communicated or disseminated causes the constituent elements of the crime not to be met, producing the same effect as the cause of non-imputability due to error. The situation derogates from the general rule in the matter (according to which error is not confused with doubt, the latter assuming that the perpetrator is aware that he cannot represent his reality correctly, in which case he should not act, and if he still goes to action – although he is aware of the insecure knowledge of the reality – will be held criminally liable for the deed committed, because he accepted the production of the socially dangerous result, thus acting indirectly). In other words, the criminal act that we analyse will be commit the crime only if the subject who knows the false nature of the data, news, information or documents that he spreads, but not the person who doubts the truth value of them, even though, under objective report, they are not real. Thus, an older orientation of the doctrine and jurisprudence is transposed into the legislative plan, which stated that the criminal law does not sanction the communication or dissemination of data or information only for the simple reason that their truthfulness has not been confirmed, but takes into account*

[21] Art. 404, the New Penal Code of Romania.

[22] Tudorel Toader, Maria-Ioana Michinici, Anda Crişu-Ciocîntă, *Noul Cod penal: comentarii pe articole*, Editura Hamangiu, Bucureşti, 2014, p. 605.

the false data or information, as well as forged documents, so that the perpetrator could not be held criminally liable for publishing data, information or documents whose authenticity was not able to know it"[23].

However, because such a circumstance, where criminal wrongdoing cannot be proven, it has a negative impact on society, visible to everyone, not just experts, fake news should be treated as a threat to national security, where threat is understood as *"external acts of commission or omission, intended and objectified in facts, situations, circumstances that outline a state of danger or harm the values that circumscribe the concept of national security, defined as such by the law on national security of Romania, respectively the state of legality, balance and social, economic and political stability necessary for the existence and development of the Romanian national state as a sovereign, unitary, independent and indivisible state, maintaining the order of law, as well as the climate of unrestricted exercise of fundamental rights, freedoms and duties of citizens, in accordance with the democratic principles and norms established by the Constitution"*[24].

In a specialized article regarding the manifestation and impact of fake news in Romania, it is stated that *"the fake news encountered in the local media landscape or on socialization platforms can be classified according to their stakes:*

a. strategic – used as part of the informational offensive of a state or an organization, in order to manipulate the population, in order to activate it in support of ideas or, on the contrary, to produce a state of apathy, disinterest, mistrust, disappointment;
b. materials – strictly aims at obtaining financial gains.

Although the concept is often associated with the fake news broadcast involuntarily, a correct approach implies the delimitation of fake news from false news, under the aspect of intention, in the case of fake news, the false information is disseminated to mislead public opinion. One of the most common prototypes

[23] Decizia Curții Constituționale no. 273/2000 referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 168 din Codul penal (M.Of. no. 101 on 28 February 2001), https://lege5.ro/Gratuit/gezdmnrzgi/art-404-comunicarea-de-informatii-false-codul-penal?dp=gqytsojwge3te, retrieved on 09.15.2019.

[24] Doru Ioan Cristescu, Doru Ioan Cristescu, Victor Cătălin Enescu, *Cadrul general tactic al investigației penale în cazul infracțiunilor contra securității naționale și acte de terorism. Ep. 3. Amenințările la adresa securității naționale. Corespondența cu infracțiunile contra securității naționale și acte de terorism. Formele de realizare a amenințărilor la adresa securității naționale. Cunoașterea căilor, metodelor și mijloacelor folosite pentru comiterea de amenințări contra securității naționale/infracțiuni contra securității naționale sau acte de terorism*, 09.03.2015, https://www.juridice.ro/364621/cadrul-general-tactic-al-investigatiei-penale-in-cazul-infractiunilor-contra-securitatii-nationale-si-acte-de-terorism-ep-3-amenintarile-la-adresa-securitatii-nationale-corespondenta-cu-infractiun.html, retrieved on 09.15.2019.

of fake news at the local level corresponds to the tabloid, sensationalist style, focused on the publication of clickbait news (with shocking titles that do not support the content), which contain exaggerations and do not cite the source of the information. They aim to increase the number of hits and, implicitly, the popularity and earnings of the source.

Failure to comply with the drafting rules may result in dangerous situations in which publications focused on obtaining useful materials from promoting fake news become, without awareness, a spokesman for entities that disseminate such news as part of the information offensive against the Romanian state"[25].

Even though fake news has all the characteristics of a threat to national security, and the phenomenon of fake news has been manifesting since the beginning of the mid-2000s, in Romania's security and defence strategies, it does not appear as part of cyber threats. Romania's current defence strategy draws attention to cyber threats only as actions launched by hostile entities, state or non-state, on information infrastructures of strategic interest of public institutions and companies[26].

Fake news that affects the country's national interests is promoted on the Romanian online, but no matter how much the authorities intervene, they will never be able to fulfil the responsibility of the citizen to filter the information he or she receives.

In 2013 and 2014, in the online environment, articles were promoted that gave as the cause of earthquakes in Galati County (located in the Predobrogean Depression, the seismogenic area with moderate seismic activity (Mw <5.3)[27], the start of shale gas exploitation by the hydraulic fracturing method. For example, on the *financial.ro* site was posted on 10.07.2013, an article stating that *"The method of exploiting the deposits in those areas is that of hydraulic fracturing, a method forbidden in most European states because of its danger posed to the environment"*[28]. In 2013, only France (2011) and Bulgaria (2012) had banned

[25] Grigore Iuliana, Andrada Halgaş, *"Fabricate" pentru România. Interese ascunse în ştirile false*, 09.01.2019, https://intelligence.sri.ro/fabricate-pentru-romania-interese-ascunse-stirile-false/, retrieved on 09.15. 2019.

[26] *Strategia națională de apărare a țării pentru perioada 2015 - 2019 – O Românie puternică în Europa și în lume,* București, 2015, para. 54, p.14.

[27] See https://ro.wikipedia.org/wiki/Seismicitatea_Rom%C3%A2niei#Depresiunea_Predobrogean%C4%83, retrieved on 16.09.2019.

[28] See https://financiarul.ro/2013/10/07/cutremurele-romanesti-cauzate-de-inceperea-exploatarii-gazelor-de-sist/, retrieved on 16.09.2019.

this type of resource exploitation[29]. The same article took some of the data from a news report posted on the Reuters site that cited a study by American geologists. But the above-mentioned study[30] refers to enhanced remote earthquake triggering at fluid-injection sites in the Midwestern United States as a consequence of large magnitude earthquakes in areas such as Japan or Chile.

A *"national debate"* started in the media, but the correct and objective information of the panicked citizens, who organized protests requesting the resignation or the sanctioning of some authorities[31], did not take place, and the exploitation was stopped[32].

Maybe, following the recent events that have disturbed the stability and balance of international allies and partners of Romania, and also Romania, the political and strategic decision makers will address this phenomenon that has such profound implications for the nation in the new Security Strategy. The inclusion of such a complex cyber threat would enable the institutions responsible for achieving national security to support, within the limits of legal competences, the documentation, even criminal, of such acts and would support the effort of the autonomous administrative authorities (The Audiovisual National Council, AGERPES) to keep traditional and digital media as much as possible, closer to the values of democracy and respect for human rights and fundamental freedoms.

BIBLIOGRAPHY

1. ***, Academia de Științe ale Securității Naționale, *Elemente conceptuale pentru fundamentarea noii strategii naţionale de apărare a ţării, Bucureşti*, 2015.
2. David Coast, Jo Fox, *Rumour and Politics* in History Compass no. 13/5, John Wiley & Sons Ltd. 2015.
3. Ben Frampton, *Clickbait: The changing face of online journalism*, BBC news, 14 September 2015.
4. Michele Kennerly, Damien Smith Pfister, *Ancient Rhetoric and Digital Networks*, The University of Alabama Press, Tuscaloosa, 2018.

[29] See https://www.reuters.com/article/us-science-fracking-earthquakes/study-raises-new-concern-about-earthquakes-and-fracking-fluids-idUSBRE96A0TZ20130711, retrieved on 16.09.2019.

[30] See http://users.clas.ufl.edu/prwaylen/GEO2200%20Readings/Readings/Fracking/Enhanced%20remote%20earthquake%20triggering%20at%20fluid-injection%20sites%20in%20the%20Midwestern%20United%20States.pdf, retrieved on 16.09.2019.

[31] *Protest spontan la Izvoarele (jud. Galati): Manifestantii cer explicatii pentru numeroasele cutremure care au afectat recent zona* https://m.hotnews.ro/stire/15719776, retrieved on 16.09.2019.

[32] See https://www.viata-libera.ro/societate/64125-chevron-renun%C8%9Ba-la-gazul-de-%C8%99ist-din-romania-o-parte-din-judetul-galati-era-concesionat-companiei, retrieved on 16.09.2019.

5. Mihai Poalelungi, *Obligaţiile pozitive şi negative ale statului prin prisma convenţiei europene pentru apărarea drepturilor omului şi a libertăţilor fundamentale*, Chișinău, 2015.
6. Stephanie Borg Psaila *Cambridge Analytica Explained: The Facts, Implications, and Open Questions,* last updated: 24 April 2018, https://dig.watch/trends/cambridge-analytica.
7. Agustin Reyna, *The Psychology of Privacy - What Can Behavioural Economics Contribute to Competition in Digital Markets?*, International Data Privacy Law, 2018, Vol. 8, No. 3.
8. Jamie Susskind, *Politica viitorului. Tehnologia digitala si societatea*, Editura Corint, București, 2019.

BENEFITS AND RISKS IN THE FIELD OF ARTIFICIAL INTELLIGENCE

Petru-Viorel ENE, PhD

Department for Parliament Liaison and Personnel Welfare, Ministry of National Defence

Starting as a great science fiction movie topic, Artificial Intelligence has already begun to impose itself on our society. If until recently it was not an extended phenomenon but rather a desideratum, a goal that seemed almost impossible to achieve, now things have changed. Artificial Intelligence has been on everyone lips in the last few years.

We take advantage of its benefits whether we speak of automated responders and online customer support, smart personal assistants, autonomously-powered self-driving vehicles or autonomous military systems. However, the technology is still in its infancy. Although the progress made in this field is extraordinary, it is time to take into account how much of an effect this technology will have on our future.

Keywords: artificial intelligence, progress, technology, autonomy, safety.

INTRODUCTION

Nearly everywhere we look today, we see intelligent systems talking to us, like *Siri* or *Alexa*, offering recommendations – *Netflix* and *Amazon*, providing financial advice and winning game shows. And we see systems emerging to improve voice recognition, image interpretation, face recognition, and even driving cars, based on techniques such as Google and Facebook's *deep learning efforts.*

Technology and humans are becoming co-workers. We rely on technology like never before. We use it to stay in touch, complete work, get the news, shop for groceries, manages our finances.

But, in order to speak about Artificial Intelligence (AI) we must see what this concept represents. There are many ways to define the field of AI. In one opinion, AI is the study of the computations that make it possible for a machine to perceive, reason and act. So, we must emphasis those three main goals[1]. Over the stretch of time, this definition has become more complex. So, in other opinion, is a subfield of computer science aimed at the development of computers capable of doing things that are normally done by *people* – in particular, things associated with people acting intelligently[2].

Mobile phones, e-commerce tools, navigation systems and many other different sensors constantly gather data or images. AI, particularly machine-learning technologies, can learn from this torrent of data to make predictions and create useful insights.

Artificial Intelligence can significantly improve people's lives and bring major benefits to our society and economy through better healthcare, more efficient public administration, safer transport, a more competitive industry and sustainable farming. AI can be used to make more accurate and faster medical diagnoses, carry out dangerous and repetitive tasks and free up valuable time. It can also help in the fight against cybercrime and minimise the use of electricity.

Some AI systems are designed around specific tasks (often called *narrow AI*) and some are designed around the ability to reason in general (referred to as *broad AI* or *general AI*). As with strong and weak AI, the most visible work tends to focus on specific problems and falls into the category of *narrow AI.*

The major exceptions to this are found in emerging work such as Google's deep learning (aimed at a general model of automatically learning categories

[1] Patrick Henry Winston, *Artificial Intelligence – Third Edition*, Addison-Wesley Publishing Company, 1993, p. 5.
[2] Cristian Hammond, *Practical Artificial Intelligence for Dummies*, Ed. John Wiley & Sons, New Jersey, 2015, p. 5.

from examples) and IBM's Watson (designed to draw conclusions from masses of textual evidence). But in both of these cases, the commercial impact of these systems is far from being at its peak. The power of narrow AI systems is that they are focused on specific tasks. The weakness is that these systems tend to be very good at what they do and absolutely useless for things that they do not do[3].

In May 2017, Google revealed AutoML, an automated machine learning system that could create an artificial intelligence solution without the assistance of a human engineer. *IBM Cloud* and *Amazon Web Services (AWS)* offer machine learning solutions that do not require AI developers[4].

We are witnessing a huge progress in this field so, in near future, we will be part of a complete new world, with AI machine everywhere, robots and lots of programmes designed to help us in our daily work but for our security as well.

When it comes to citizen's security, we have to mention that there is a need for face recognition in our daily life, in order to maintain our community safe. Airline companies, in collaboration with the governments around the world, have been working to implement biometric face scanners in domestic airport for better streamline security.

Well, if on the one hand we have to recognize that this measure can represent an important step in our travel security, on the other hand, we must consider all the complications that may occur after such a measure will be implemented in airport across the world and on every street. Artificial Intelligence represents a great step for our technological development. Unfortunately, this type of new technology brings with it, besides opportunities, serious questions concerning citizen's privacy.

In the following we will be addressing this issue with the purpose of creating a picture of the artificial intelligence impact.

HUMANIZING TECHNOLOGY – THE FUTURE OF OUR SOCIETY

Even though this subject can look easy to approach, we have to consider that our society is involved with technology that we do not even realize how much it affects our daily lives and that it is actually changing our brains and our way of life.

If we are searching for a start in this field, we can observe that, the concept of Artificial Intelligence was coined by John McCarthy[5] in 1956 when he held the first academic conference on the subject. Five years later Alan Turing[6] wrote a paper

[3] *Ibidem*, p. 6.

[4] Denis Rothman, *Artificial Intelligence by Example*, Packt Publishing Ltd, Birmingham, 2018, p. 8.

[5] 4 September 1927 – 24 October 2011 – John was a legendary computer scientist at Stanford University who developed time-sharing, invented LISP, and founded the field of Artificial Intelligence, see http://jmc.stanford.edu/, retrieved on 06.09.2019.

[6] Performed a test of a machine's ability to exhibit intelligent behaviour equivalent to, or indistinguishable from, that of a human, more on https://www.turing.org.uk/scrapbook/test.html, retrieved on 16.09.2019.

on the notion of machines being able to simulate human beings and to do intelligent things, such as to play Chess. Since then, this technology has made considerable progress.

If, at the beginning, this layout raised a lot of questions, now, computer's ability to recognize people, to act in a way or another, to search or to talk to us is extraordinary. But what has led us to want this type of technology to be part of our life?

The history of Artificial Intelligence began in antiquity, with myths, stories and rumours of artificial beings endowed with intelligence or consciousness by master craftsmen. The seeds of modern AI were planted by classical philosophers who attempted to describe the process of human thinking as the mechanical manipulation of symbols. But is this philosophical appeal enough for modern man to create a technology that helps us to do things we have only dreamed of doing?

Artificial Intelligence is a strong incentive for us in order to develop a totally different society in which our routine work can be done by robots, to progress faster than ever and to reduce the manpower costs. We need AI because the work that we need to do is increasing day-to-day. Therefore, it is a good idea to automate the routine work. This saves the manpower of the organization and also increases the productivity.

Additionally, through Artificial Intelligence, the company can also get the skilled persons for the development of the company. Moreover, the companies today think that they want to mechanize all the regular and routine work.

In the recent years, Artificial Intelligence has been advancing much quicker than before, and today, we use AI many times during a day – often, without even realizing it.

From voice-powered personal assistants to more underlying and fundamental technologies such as behavioural algorithms, there are several examples and applications of artificial intelligence in use today.

A true artificially-intelligent system is one that can learn on its own. We are talking about neural networks like of Google's DeepMind, which can make connections and reach meanings without relying on pre-defined behavioural algorithms. True AI can improve on past iterations, getting smarter and more aware, allowing it to enhance its capabilities and its knowledge[7].

Thanks to the advances of machine learning that have revolutionised the field, AI now works completely different than before. Previously, engineers needed to code each rule such as *if this then that*, but now computers can learn from examples and figure it out the rules on their own without being explicitly programmed using

[7] See https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificial-intelligence-in-use-today/# 68c44420de57, retrieved on16.09.2019.

sources as varied as text, images, video and speech. If given enough data, machine learning algorithms can predict, personalise, recognise and uncover structure in the data to provide insights or identity anomalies[8].

The finest example of learning machine is probably the *Fish Brain Experiment*. This neuronal interfacing experiment has proven that the reaction of a brain can be forecasted and that a brain works no matter if the stimulus is artificial or natural.

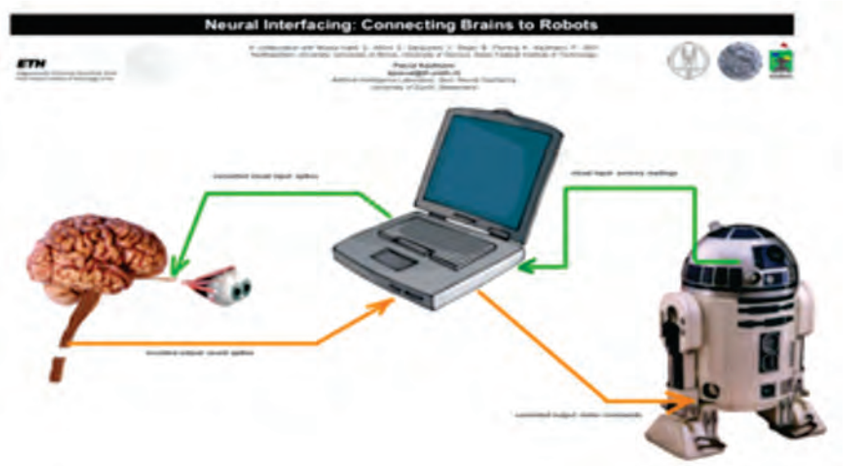


Figure no. 1: Fish Brain Experiment

The idea consists in connecting a fish brain to a robot. The optic nerve is cut from the eyes and connected to the robots' camera which provides the stimulus for the brain (input) to react. The spinal cord is also cut and connected with the bot. The spikes measured at the end of the spinal cord are transformed in action signals for the bot (output).

- The bot was stimulated by light beams and the expected reaction was that it would move in a forecasted direction. The following scenarios have been tested:
- Forward – The bot is attracted by light. The expected result is that there will be a forward movement;
- Right – The bot is stimulated by a light beam on its left and therefore will move the right wheel faster in order to balance his body and align to the light beam (remember that the bot thinks to be a fish and therefore will stabilize his position to front face the light);
- Left – The bot is stimulated also on its right and therefore will move the left wheel faster;

[8] See https://uxdesign.cc/ai-today-definition-what-is-ai-for-risks-and-unexpected-consequences-on-society-3eda9b78a37a, retrieved on 16.09.2019.

- Escape – The bot is programmed to avoid/escape the light, the expected result is that it will stop moving or deviate[9].

This is only a fraction of what Artificial Intelligence means and what progress and tests we make in this field. Such tests are meant to clarify our path in this permanent technological expansion but even so, we must emphasize that AI is part of our daily life. In fact, basic things like our e-mail address use AI. Google uses AI to ensure that nearly all email landing in your inbox is authentic. Their filters attempt to sort emails in some categories in order to help us to find our way to important communications quicker.

More, Gmail's *nudging* feature reminds you to follow up on the emails you have ignored or forgotten. Using AI, Gmail attempts to determine which emails require a response, then highlights them after a few days of non-attention. Probably, the best-known fingerprint of AI is the Google predictive search. When you begin typing a search term and Google makes recommendations for you to choose from, that is AI in action.

We have mentioned all these aspects in order to have a solid idea about what kind of impact AI has in our life. Although we see that big companies are using this technology, we must say that Artificial Intelligence has the potential to offer $15.7 trillion to the global economy by 2030. All those times Amazon recommends a book or Netflix suggests a film are based on algorithms that examine what we have bought or watched. The algorithms learn from those purchases, using them to suggest other things we might enjoy. AI lies behind those algorithms.

Maybe for some consumers this kind of aggressive publicity advertising is not the best way to live but, there are a lot of people that are buying all kind of stuff because of this type of suggestions.

Not only Google, Amazon or Facebook are using AI but financial companies too. Consider how many people have a bank account. According to a research run by the World Bank, globally, 69% of adult population have an account[10]. Financial companies often use artificial intelligence to monitor transaction requests since algorithms process information so quickly. They spot patterns in our transactions and alert users to suspicious activity.

Have you flown in a plane? If the answer is yes, I must tell you something. An average Boeing 777 pilot spends just seven minutes manually piloting the plane. An Airbus plane pilot manages half of that. The airplanes use a combination of motion sensors and GPS to track their position in flight. The software can even land commercial aircraft, though much of those seven minutes is spent on takeoff

[9] See https://www.hwzdigital.ch/artificial-intelligence-where-are-we-today/, retrieved on 16.09.2019.
[10] See https://globalfindex.worldbank.org/, retrieved on 16.09.2019.

and landing. This is the best use of the technology, where the impact of artificial intelligence in everyday life is barely felt[11].

As we mention before, compared to other fields such as Mathematics or Physics that have been around for centuries, AI is relatively in its infancy. Over the last couple of decades, AI has produced some spectacular products such as self-driving cars and intelligent robots that can walk.

Based on the direction in which we are heading, it is pretty obvious that achieving intelligence will have a great impact on our lives in the coming years.

Let us think about how the human brain manages to do so much with such effortless ease. We can recognize objects, understand languages, learn new things, and perform many more sophisticated tasks with our brain. How does the human brain do this? When you try to do this with a machine, you will see that it falls way behind! For example, when we try to look for things such as extra-terrestrial life or time travel, we do not know if those things exist. The good thing about the fundament of AI is that we know it exists. Our brain is the main pillar in this field! It is a spectacular example of an intelligent system. All we have to do is to mimic its functionality to create an intelligent system that can do something similar, possibly even more.

We see that the main objective regarding AI and how this technology might be used, is to create a super brain, capable of far more than the people's brain. Imagine a total new mind with the ability to take complex decisions in fraction of a second. This type of technology will be a real treasure for our security, for our defence system.

So, for our benefits and in order to reach new standards in this field, we need to design and develop intelligent machines that can do the work of a human brain better and faster. We need AI systems that can handle large amounts of data in an efficient way, ingest data simultaneously from multiple sources without any lag, index and organize data in a way that allows us to derive insights, learn from new data and update constantly using the right learning algorithms, think and respond to situations based on the conditions in real time[12].

We must consider the fact that this technology will be at the foundation of our future society because both private and public sectors embrace its benefits and everybody is trying to implement this new way of co-working between man and AI machines.

All major companies are using AI in the battle against cyber-attacks. The application of artificial intelligence, in particular machine learning, to cyber operation, promise to offer more efficient and more effective tools for carrying out attacks that occur.

[11] See https://www.forbes.com/sites/forbestechcouncil/2018/03/07/the-impact-of-artificial-intelligence-in-the-everyday-lives -of-consumers/#61ace7826f31, retrieved on 16.09.2019.

[12] Prateek Joshi, *Artificial Intelligence with Python,* Packt Publishing, Birmingham, 2017, p. 11.

The most time-consuming cyber-attack preparation tasks, like sifting through large amounts of data in search of vulnerabilities in software to exploit or creating better spear phishing campaigns, will no longer require time and deep pockets to pay for human labour, but will occur constantly and quickly.

Machines do not need to pause for breaks and will not suffer from fatigue or weariness that might allow them to miss a potential vulnerability or exploit. The ability to synthesize unstructured data will allow machines to make potential connections that might be blind to the human eye, or at a minimum would not be immediately obvious[13]. This is an important reason for a company to start using this resource in order to secure their data and also to reduce their costs.

But, in this area, there is a constant concern for every developed country regarding this technology. For example, the European Union (EU) is facilitating and enhancing cooperation on AI across the Union to boost its competitiveness and ensure trust based on EU values. Its approach to AI and robotics deals with technological, ethical, legal and socio-economic aspects to boost the EU's research and industrial capacity and put AI at the service of European citizens and economy. These measures become a reality through massive investments.

In this respect, the European Commission has already invested significant amounts in artificial intelligence in 2014-2020 period, cognitive systems, robotics, big data and future and emerging technologies to help Europe be competitive. The picture below gives us a categorical conclusion: AI represents a priority at EU level[14].

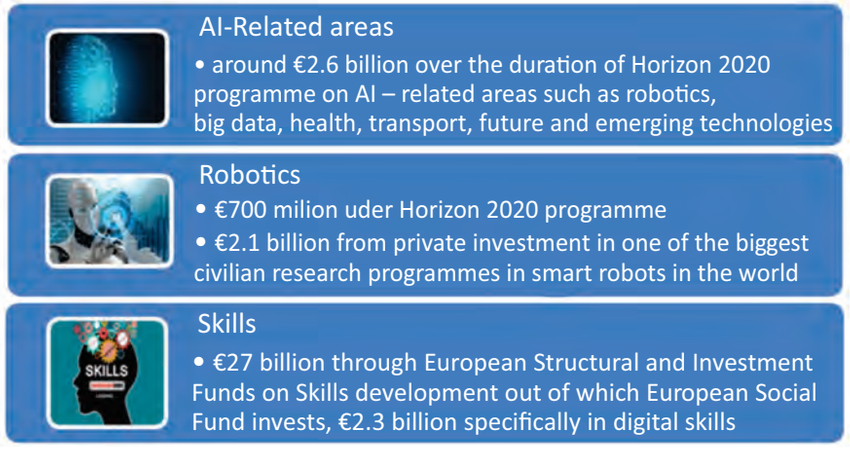


Figure no. 2: Artificial Intelligence for Europe

[13] See https://www.weforum.org/agenda/2019/04/how-ai-raises-the-threat-of-cyberattack-and-why-the-best-defence-is-more -ai-5eb78ba081, retrieved on 16.09.2019.

[14] See https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe, retrieved on 17.09.2019.

Artificial Intelligence has become an area of strategic importance and a key driver of economic development. It can bring solutions to many societal challenges from treating diseases to minimising the environmental impact of farming.

Moreover, the European Commission and the Member States published a Coordinated Action Plan on the development of AI in the EU on 7 December 2018 in order to promote the development of Artificial Intelligence (AI) in Europe.

The Coordinated EU Plan is needed because only when all European countries work together, we can make the most of the opportunities offered by AI and become a world leader in this crucial technology for the future of our societies. Furthermore, cooperation between Member States and the Commission is essential to address new challenges brought by AI[15].

We notice that AI with its full implication on our society is a priority for governments and, of course, for private sector. Given that our data and our work are migrating in this digital world, it is a great way to use this new technology in order to create a safe on-line environment and, at the same time, to reduce our work. We aim to implement all of this and by doing so, to create a new way of life, based on technology even more, with automatic machines designed for immediate response.

All these goals that we want to accomplish are undoubtedly of enormous significance for our economy and four our life in general. This amazing technological progress gives us the chance for a better future. But does this technology involve only benefits? What are the implications of all of this in the field of security?

SECURITY CHALLENGES IN THE FIELD OF ARTIFICIAL INTELLIGENCE

It is clear to everyone that we are witnessing a great progress and we can use this technology for our well-being and for a more comfortable life. But, like any great innovation with huge impact, there is the possibility to use it in a way in which it can lead to lack of privacy or even insecurity. We highlight this type of problems because their impact on our life and our society, has the capacity to create real problems.

Let us take a look on the AI impact in security field. AI and machine learning can redefine every aspect of our security today. From improving the organizations' ability to anticipate any attack that can occur to securing the perimeters of any military base, this technology represents an important pillar in defence and security worldwide.

[15] European Commission – Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Coordinated Plan on Artificial Intelligence*, Brussels, 2018.

As we can see, in the competition to lead the emerging technology race and the futuristic warfare battleground, artificial intelligence is rapidly becoming the centre of the global power play. The development in autonomous weapons system (AWS) is progressing rapidly, and this increase in the weaponization of artificial intelligence seems to have become a highly destabilizing development.

Of course, that is a great way to secure our soldier and to reduce casualty, but this brings complex security challenges too, not only for each nation involved but also for the future of humanity. This will sound a little too extreme, but a weapon system that, once activated, can select and engage human and non-human targets, without further intervention by a human designer or operator, is an issue that inspires fear.

If until now we could not conceive that an automatic machine can engage in battle actions, now this machine has the ability to perform warfare task without any human involvement and intervention, using only its sensors, programmes and algorithms.

The rapid development of AI weaponization is evident across the board: navigating and utilizing unmanned naval, aerial, and terrain vehicles, producing collateral-damage estimations, deploying *"fire-and-forget"* missile systems and using stationary systems to automate everything from personnel systems and equipment maintenance to the deployment of surveillance drones, robots and more are all examples.

In this context, we have to outline rules in order to use AI without creating even greater devastation than our traditional weapon and, additionally, to see if there is auspicious to allow or restrict it. Let us take an example. Now, an AI machine in war operations is first programmed to determine the nature of the danger. The intention is that AI machines should begin programming itself. In this case, how will human control the weaponization of AI? When and if an autonomous system kills, who is responsible for the killing?[16]

Everyone knows that being a soldier is a dangerous job, but some of the tasks that soldiers are required to do are unbelievable: clearing out hostile building, deactivating unexploded bombs. What if we could send robots to do these jobs instead of humans? If something went wrong, we would only lose money not life. We see a lot of benefits of this amazing technology but are we sure that this will not affect our entire way of life?

The United States of America is already using unmanned aerial vehicles to conduct surveillance and drop missiles on terrorists target overseas[17]. The efficacy

[16] See https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/#4877c372368 6, retrieved on 17.09.2019.

[17] See https://science.howstuffworks.com/robots-replacing-soldiers1.htm, retrieved on 17.09.2019.

is amazing but there are controversial discussions about the morality of those actions. While drones do their work from high above, the enemy does not stand a chance. It is true that, in this scenario, human controllers decide when these drones will fire. Even so, is it a problem of proportionality or not?

Even though those *lethal autonomous weapons* have not been used yet, we have to see the entire picture and to analyse the risks because the technology will finally replace the human with an algorithm that makes the decision. The algorithm could have a fixed list of people it can target and fire or it could be trained to predict if it is necessary to engage. But can we trust a machine to protect us?[18]

So, if we are talking about security and the way in which AI can influence this area, we have to take in consideration some facts. If now we are at the beginning of this technology, applications of AI in defence can further be extended to designing targeted missiles, sophisticated weapons, and intensive fighter planes. These applications, which require thorough research, hold the potential to revolutionize the face of defence in the near future[19].

Let us take the best-known example. The popularity of *military drones* has skyrocketed in the recent years. Drone technology has come a long way since its inception and is now finding application in unmanned military aerial vehicles. But this type of technology is also used in extremely concerning attacks[20] so we must weigh the benefits and risks too.

Maybe military actions do not represent a field that interests us daily, although it should. Then, let us talk about *facial recognition technology*. Those scanners are already at some airports and in towns around the world. It is understandable that government agencies are aiming to improve efficiency when it comes to the way citizens are travelling, but is this type of surveillance legal or not really?

The airlines companies want to implement this technology in order to save money, time and to secure their flights. How does this process work? A camera takes you a photo and then the Customs and Border Protection's (CBP) traveller verification service matches it to a photo of the agency responsible in your country with this kind of issue. These could be images from sources like passports or other travel documents. This process is great because, ideally, it will replace the manual checking of passports nationwide. But do we have to be concerned about privacy? By consenting to the facial recognition, the government can create a digital identity for you and track you without your consent or knowledge. While they may not be

[18] See https://www.vox.com/2019/6/21/18691459/killer-robots-lethal-autonomous-weapons-ai-war, retrieved on17.09.2019.

[19] See https://www.forbes.com/sites/cognitiveworld/2018/08/26/4-ways-the-global-defense-forces-are-using-ai/#478bed10 503e, retrieved on 17.09.2019.

[20] See https://www.bbc.com/news/world-middle-east-49721301, retrieved on 17.09.2019.

using that power right now, there is a lack of regulation preventing them from using it that way[21].

But facial recognition has other key issues, as technical problems. According to a Homeland Security watchdog, from the USA, the facial recognition systems used at airports *only worked 85% in some cases*[22]. Can this percentage create real problems when it comes to passenger security? Probably unspeakable issues if we are thinking of the risk involved in letting a terrorist in a plane.

This technology is already seeping into everyday life, and the increased regularity with which Americans encounter facial recognition as a matter of course while traveling will reinforce this familiarity; in this context, it is easy to imagine content from a government-operated facial recognition database being utilized in other settings aside from airports – say, for example, monitoring peaceful protests.

If for some people this technology is great and carries important benefits, there are citizens concerned about their privacy. They argue that a true secure environment for everyone must be maintained by police not by AI machines. Frequently, they are invoking studies showing that facial recognition technology is more likely to misidentify people of colour, young people and women, leading to them being stopped incorrectly. Their conclusion is trenchant: facial recognition technology has no place on our streets – it must be banned[23].

In China, about 200 million surveillance cameras are scattered around the country. In fact, nearly every one of its *1.4 billion citizens* is in China's facial recognition database. Of course, AI companies believe surveillance and face recognition technology will make the country safer, but civil liberties advocates believe the issues of error and privacy may outweigh the security value[24].

And maybe they are right. Let us focus on this scenario: a suspect of terrorism setting off on a suicide mission in a densely populated city centre. If his plan becomes a reality, we are talking about hundreds of victims. In this case, the face recognition programme picks him up and automatically compares his features to photos on a database of known terrorists or *"persons of interest"* to the security services. The system triggers the alarm and in a couple of seconds the best anti-terrorist force neutralize the suspect before he blows himself up. But that is great, you can say. Now let us imagine that the facial recognition tech was wrong and that team killed a child with a black backpack. An innocent life would have been summarily snuffed out because we put too much faith in a fallible system[25].

[21] See https://eu.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everythin g-you-need-know/1998749001/, retrieved on 17.09.2019.

[22] See https://techcrunch.com/2019/05/13/americans-opt-out-facial-recognition-airport/, retrieved on 17.09.2019.

[23] See https://www.libertyhumanrights.org.uk/resist-facial-recognition, retrieved on 17.09.2019.

[24] See https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html, retrieved on 17.09.2019.

[25] See https://www.bbc.com/news/business-48842750, retrieved on 17.09.2019.

We see that there are different opinions in this field and every side has good arguments but in this technological wave we need, more and more, to create a legal framework in order to create a secure environment for our citizens.

CONCLUSIONS

From the foregoing, we can say that, both at the level of public and private sector, AI will become an important phenomenon with huge impact in our most relevant actions. If we manage to create the legal framework in this field, we will be able to improve our life and to avoid any unfortunate consequence.

We can say that we are witnessing the golden age of AI. It is the era of research, experimentation innovation, in this field. With all this remarkable success on the cards we are still very far from creating the perfect AI but it is clear for everyone that the impact is huge. Whether we are on the side of those who support AI progress or not, we have to take into account the progress that we have made and the fact that we can face, not infrequently, certain hazards.

Right now, this kind of technology is fairly new, but it is becoming more complex day by day. It is a great way to improve our life and to be sure that, for certain jobs, we have the capacity to use machines in order to eliminate any risk for our citizens. But, once we consider AI machines as entities that can perceive, feel and act, we have to solve the legal problem, we must create an appropriate legal framework. Should this tech be treated like animals, humans or machines?

We consider that it is mandatory to have an ethical code and clear rules related to artificial intelligence, both for those who develop and use such machines in order to be sure that their purpose is a peaceful one, that they create AI machines for our help.

Furthermore, AI will not live very long if the public loses confidence in it, because there is an opinion among us that AI could grow so immensely strong that it would be difficult for humans to control. So, establishing citizens' confidence is a step that we must follow.

Artificial Intelligence has a great potential, it brings huge economic benefits and protect our citizens. But we have the responsibility to implement this tech in accordance with ethics and moral code.

BIBLIOGRAPHY

1. ***, European Commission – Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Coordinated Plan on Artificial Intelligence*, Brussels, 2018.
2. Cristian Hammond, *Practical Artificial Intelligence for Dummies*, John Wiley&Sons, New Jersey, 2015.

3. Prateek Joshi, *Artificial Intelligence with Python*, Packt Publishing, Birmingham, 2017.
4. Denis Rothman, *Artificial Intelligence by Example*, Packt Publishing Ltd, Birmingham, 2018.
5. Chris Smith, Brian McGuire, Ting Huang, Gary Yang, *The History of Artificial Intelligence*, University of Washington, 2006.
6. Patrick Henry Winston, *Artificial Intelligence – Third Edition*, Addison-Wesley Publishing Company, 1993.

WEBOGRAPHY

1. https://www.bbc.com/news/business-48842750
2. https://www.bbc.com/news/world-middle-east-49721301
3. https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html
4. https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe
5. https://eu.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everythin g-you-need-know/1998749001/
6. https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/#4877c3723686
7. https://www.forbes.com/sites/forbestechcouncil/2018/03/07/the-impact-of-artificial-intelligence-in-the-everyday-lives -of-consumers/#61ace7826f31
8. https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificial-intelligence-in-use-today/# 68c44420de57
9. https://globalfindex.worldbank.org/
10. https://www.hwzdigital.ch/artificial-intelligence-where-are-we-today/.
11. http://jmc.stanford.edu/
12. https://www.libertyhumanrights.org.uk/resist-facial-recognition
13. https://science.howstuffworks.com/robots-replacing-soldiers1.htm
14. https://techcrunch.com/2019/05/13/americans-opt-out-facial-recognition-airport/
15. https://uxdesign.cc/ai-today-definition-what-is-ai-for-risks-and-unexpected-consequences-on-society-3eda9b78a37a
16. https://www.vox.com/2019/6/21/18691459/killer-robots-lethal-autonomous-weapons-ai-war
17. https://www.weforum.org/agenda/2019/04/how-ai-raises-the-threat-of-cyberattack-and-why-the-best-defence-is-more-ai-5eb78ba081

TRENDS IN THE EVOLUTION OF HYBRID CONFLICTS

Alexandru HERCIU, PhD
Senior Lecturer, "Carol I" National Defence University, Bucharest

The risks and threats of a conventional, unconventional, asymmetrical, and cyber nature become increasingly complex and unpredictable. Their combination generates the production of apparent disturbances in the contemporary operational environment, with severe consequences on the security of the states.

A conclusion that emerges, analysing the evolution of the military phenomenon over the last thirty years, is that, in the future, both great powers and non-state actors will resort to the most different actions to reach their interests. These actions have demonstrated their efficiency through their unusual nature and the lack of effective countermeasures such as information warfare, cyber warfare, network warfare, electronic warfare, psychological warfare, or media warfare.

If the future of military action is to be marked by hybridity, states, alliances and coalitions must develop those conventional, unconventional, irregular and cyber capabilities that will ensure the planning, preparation, execution, and evaluation of operations in the full spectrum.

Keywords: hybrid threats, hybrid conflict, irregular operations, electronic warfare, psychological warfare.

INTRODUCTION

The phenomena of the military conflict will be profoundly changed, being influenced by significant developments in the international security environment and the dynamics of military operations. The latter will undergo profound transformations by introducing intelligent weapon systems and platforms, advanced sensors, modern command and control systems, as well as by digitizing the battlefield.

Therefore, military operations will be conducted in a fluid, multidimensional operational environment. Asymmetric actions will characterize the confrontational environment, in which forces will conduct combat actions with high mobility and decentralized. The forces involved will use a wide range of air, land, maritime, information, psychological, and special operations. They will be carried out simultaneously at a strategic, operational and tactical level, continually and at a sustained pace, aiming at the decisive strike of the enemy's centres of gravity and the immediate victory by its physical and psychological defeat.

The lessons learned from recent and ongoing military conflicts are concrete elements of analysis from which we can outline some trends in the evolution of military conflicts in the future, with an accent on hybrid conflicts.

FUTURE DEVELOPMENTS AND TRENDS IN HYBRID CONFLICTS

New Challenges in the Contemporary Operational Environment

The contemporary operating environment is marked by insecurity and uncertainty. Risks and threats to the security of the states and the diversity of the actors involved, generate unpredictability. This situation causes difficulties in the use of power tools for crisis management and conflict prevention[1].

In this regard, the risks and threats of a conventional, unconventional, asymmetrical, and cyber nature become increasingly complex and unpredictable. Their combination generates the production of apparent disturbances in the contemporary operational environment, with severe consequences on the security of the states.

The actors involved in shaping the contemporary operational environment have continuously been diversified and radicalized. Thus, in addition to regular armed

[1] Ion Mituleţu, *Tendinţe privind evoluţia fizionomiei acţiunilor militare*, Scientific paper, *Tactică şi artă operativă – forţe terestre (TAOFT)* Scientific Conference, Bucureşti, 2014.

forces, we encounter irregular, paramilitary, insurgent, guerrilla, terrorist, separatist, undercover forces, mercenaries, criminal organizations, government structures, and the civilian population. This fact determines a sophisticated approach to the situation in areas of strategic interest.

If we interpret the aspects of the contemporary operational environment from a political, economic, social, cultural, religious, scientific, or military point of view and we overlap the risks, threats, and actors involved, we find the diversity of situations generating instability and potentiating crises and conflicts. They must be managed according to the particularities, interests, and resources demanded to be allocated.

To these elements of analysis, we can add the proliferation of weapons of mass destruction (WMD) and the tendency to acquire and possess them by non-state actors. This reality signifies an unconventional strategic threat at regional and global level.

In the context of the comprehensive approach to the operational environment at present and in the future, the question arises whether the existence of a military doctrine that includes the concept of the use of the armed forces only for conventional operations of small, medium or high intensity is sufficient. The question that arises is whether or not it is necessary to adapt it to other varieties of situations that can be generated in the area of operations and to change the perception concerning the physiognomy of military actions.

The complexity of the military actions includes operations specific to the armed struggle, irregular operations (expressed by insurgency, guerrilla warfare, terrorism or organized crime), security, stability, and post-conflict reconstruction, peace support, humanitarian, unconventional, counterterrorism, or cyber-attacks operations. This mixture requires a realistic evaluation at the political-military and military-strategic level in order to develop a multilateral vision on the physiognomy of military actions in the present and future operational environment.

We strongly consider that the evaluation must be directed towards establishing the benchmarks, options, and resources necessary to develop a strategic vision that reflects the modalities of planning, preparation, execution, and evaluation of the military operations in their full spectrum.

Although in the military literature we find more and more theoretical expressions in which it is appreciated that the risk of a conventional armed conflict is shallow in the short term, we believe that this statement will have to be reassessed. Even if the risk of a conventional military confrontation is latent, it may be exacerbated. Various situations, such as the activation of frozen conflicts, the increase of territorial, cultural and religious tensions, the competition for vital resources, for food, as well as the unequal population growth in different regions and its tendency to migrate can lead to crisis or conflict situations.

In this context, the emergence of critical situations in the operational environment, which generates crises, which cannot be managed through the use of political, diplomatic and economic power instruments, can be converted into multiple strategic events. They can escalate, and their solution involves activating and, as the case may be, using the military instrument, namely, the armed force.

THE CYCLICAL NATURE OF MILITARY ACTION

Historical events justify our assertion that military action is cyclical. The military action manifests itself depending on the typology of the risks and threats existing and the actors involved in the fulfilment of the established political-military objectives, according to the intentions, interests, and resources allocated.

First, the dominant conventional risks and threats are neutralized by actions specific to the armed struggle, executed in national and multinational contexts. Conventional forces participating in these types of military actions execute small, medium, or high-intensity operations in the theatre of operations (joint area of operations).

The joint and multinational operations are of military-strategic, operational and tactical level and are executed within coalitions or alliances.

The main peculiarity of this joint and multinational operations was the application of the doctrinal-strategic concept *"air-ground battle"*, which implies the integrated action in the air and ground environment, in order to fulfil the set objectives and to achieve the desired end-state.

This concept is aimed at the airspace domination, the exploitation of the radio-electronic advantages, and the manifestation of the striking power in the theatre of operations. Operation *"DESERT STORM"* carried out in 1991 in the Persian Gulf was based on the *"air-ground battle"* concept, and Operation *"ALLIED FORCES"* carried out in 1999 in Kosovo was based only on the air component of the concept, being ensured the conditions for the accomplishment of the planned missions[2].

During these major conventional operations, four action concepts were highlighted, namely the dominant manoeuvre, the selective precision engagement, the multidimensional protection, and the focused logistic. The conclusions resulting from the employment of these concepts were admitted learned lessons. They were inserted into the content of NATO military documents, including in the Romanian Armed Forces.

The revolution in military affairs was an essential step in the evolution of the physiognomy of military action. The valorisation of the technological performances ensured the transformation at the conceptual, doctrinal, organizational, and force

[2] *********Conflicte militare. Lecții învățate*, Editura Universităţii Naţionale de Apărare *"Carol I",* Bucureşti, 2010, p. 78.

procurement level. The qualitative leap ensured the production of added value by developing the network design at the mission disposal.

The network model enabled the adversary engagement in the entire area of operation and the achievement of the planned effect in relation to the established goals.

The revolution in military affairs has generated a wide range of military actions, materialized in the concepts of network-based operations, effects-based operations, information war, or cyberwar. These varieties of military actions are based on procedures specific to the armed struggle, but they integrate high-technologies. These advanced technologies ensure that information superiority is obtained, maintained, and transformed into decision superiority, and subsequently into action superiority. Possessing superiority ensures the discovery, striking and neutralization of the adversary's centre of gravity, meeting the set objectives and achieving the desired end-state.

An innovative element of the revolution in military affairs was the achievement of efficient command and control systems of the C4ISR type, incorporating advanced information, communication and computer technologies and fit equipment for discovering, selecting, and employing the targets, depending on their relevance.

The use of information superiority results marked the truly revolutionary leap in the evolution of the physiognomy of military action. Now the information is oriented towards reducing the length of the decision-making process and reducing the response time accordingly.

This concept, in our opinion, entails the fulfilment of the efficiency criterion, expressed first of all by the fact that the decision-making process considers that the response time of own forces should be shorter than the time required for the opponent to perform similar actions. By advancing the adversary cognitively and temporally, it is intended to defeat its will to fight and not to destroy/annihilate its physical strength.

"ENDURING FREEDOM" operation carried out in Afghanistan (2001) implemented the concept of Effects-Based Operations. *"IRAQI FREEDOM"* operation (2003) applied the concept of Network-Based Operations, high-tech elements being used for the first time.

In this context, we believe that the results of the revolution in military affairs founded a new culture of war at the beginning of the 21st century. The new leap produced fundamental changes in the evolution of the physiognomy of military action.

Secondly, we observed that in the theatres of operations opened at the beginning of the 21st century the military operations do not end with the achievement of the strategic objectives, moving to a new stage, the transition to post-conflict operations.

In the context of post-conflict operations, the concept of SSTR (security, stabilization, transition, and reconstruction) was introduced. This concept is aimed at creating the conditions for the support of the host nation in taking over the political power, ensuring good governance, applying measures for economic reconstruction and development, respecting the legal rules and fostering the achievement of a real democracy. The effort of these activities aiming at the transition from major combat operations to actions that facilitate post-conflict stabilization and reconstruction, becomes diffuse and uncertain, given that the objectives are gradually approached and the desired end-state cannot be clearly defined.

Another feature of post-conflict operations is represented by the diversity of the actors involved, including the civilian population. They have conflicting purposes and try to gain advantages over a stronger adversary. This fact causes the approach to the action modalities under the conditions of asymmetry.

In this respect, post-conflict stabilization and reconstruction operations are aimed at facilitating the transition to the political power taking over by the local structures, introducing the concept of asymmetry expressed in asymmetric threats, asymmetric actors, asymmetric actions.

The shock generated by the asymmetry targeted the actions of non-state actors (or factions existing in some states) to counteract the superiority of the adversary by unconventional means and to minimize the advantages of the technological gaps. These means do not respect the rules and principles of war, the rules of law, and international law.

Initially, counteracting asymmetry involved all the actions of conventional/regular forces to combat terrorism, insurgency, guerrilla warfare, and organized crime.

The stated purpose of the asymmetrical actions carried out by the non-state actors was to create uncertainty and unpredictability, on the one hand, and to exacerbate violence, on the other hand.

Thus, we can assert that the asymmetrical threats took the place of the conventional balance, and the asymmetrical actions proved violence in different theatres of operations.

The development of atypical tactics, techniques, and procedures, challenging to counter with conventional means, made it possible to convert asymmetrical conflict into irregular conflict (Irregular Warfare). The concept of irregular conflict involves a set of indirect and asymmetrical violent actions between state and non-state actors, in order to gain influence, control, and legitimacy on the civilian population of the host nation.

In this context, the irregular conflict emphasizes the essential role of the civilian population and all the actions carried out in the area of responsibility are directed towards gaining legitimacy and popular support with the civil-military available means.

The transition from operations specific to the armed conflict – considered regular operations, towards asymmetry and irregularity, has diversified the range of military actions and generated the concept of full-spectrum operations.

The main types of irregular operations include insurgency and counterinsurgency, terrorism and counterterrorism, unconventional operations involving CBRN threats management, internal security with external support, stability, security, transition and reconstruction operations, civil-military operations, psychological operations, information-based operations.

The multidimensional approach (in which the effort is shifted from conventional to unconventional actions) changes the perception on the physiognomy of the military operation. The superiority of the belligerent force and the control of the occupied territory no longer have the same relevance. The conflict under the given conditions will not end in a short time, the consumption of resources will increase, and the political-military goals will be challenging to achieve.

WHICH WILL BE THE PHYSIOGNOMY OF MILITARY ACTION IN THE FUTURE?

In the future, we consider that there will be a new transition, this time in the opposite direction, from asymmetry and irregularity to the operations specific to the armed conflict (combat type). This change entails the application of the JIM concept, described by the joint, inter-agency, and multinational combination.

These operations will integrate conventional and unconventional actions, depending on the nature of the risks and threats in the operational environment and will incorporate the achievements of the knowledge era.

The evolution of the military actions will be directed to operations specific to the armed conflict. Command and control systems, the combined forces structure, the multidimensional protection, and the logistical support must ensure the manifestation of the combat power in the entire area of operations and guarantee the achievement of the strategic objectives and the desired end-state.

When conventional risks and threats integrate unconventional and cyber vulnerabilities, armed combat operations will combine conventional, unconventional, irregular, and cyber actions, resulting in a hybridization of conflict.

Hybrid operations, in which the combined capabilities are very well defined, will be concentrated in areas of strategic interest. These areas include, among

other things, vital resources, critical infrastructure elements, energy lines and strategic communications, frozen conflicts, territorial, cultural and religious disputes whose settlement involves the use of the military instrument.

In this regard, we believe that future military operations will be short-term, but of high intensity. They will be limited to the disputed area, highlighting the JIM concept, but with the temporal and spatial insertion of unconventional, irregular and cyber actions.

The future war is a war whose essential feature is given by the indirect action supported by one or both sides involved in the conflict. The hypothesis is supported by explanations regarding the characteristics of a local or limited hybrid war. Thus, cyber-attacks, actions of economic control, purchase of political power, corruption, the transformation of the population of the adversary state into a real fifth column, actions in the sphere of environmental protection are solid arguments in describing the physiognomy of a hybrid war[3].

As the recent conflicts have shown, cyberattacks on the information systems preface any other form of action and aim to block economic, military, and security activities as well as collecting information on military and economic capabilities. The cyberattacks are materialized by actions carried out in order to trigger a controlled social disorder and to exacerbate the dissatisfaction of the civilian population with the inability of the state authorities.

The war in Ukraine has revealed a new facet of hybridity, meaning that military action can be carried out by an *"undercover"* army.

In conclusion, given the consequences of a future war between two great military powers, we consider that this is possible only in the form of a hybrid war, in which the governmental responsibility of the belligerents is minimal and does not imply recourse to the nuclear arsenal. Also, it is unlikely that this type of war will take place on the territory of a great power, but on the geographical space of one or more allies of a party[4].

If the future of military action is to be marked by hybridity, states, alliances and coalitions must develop those conventional, unconventional, irregular and cyber capabilities that will ensure the planning, preparation, execution, and evaluation of operations in the full spectrum.

The *"Smart Defence"* concept can be a way of applying the principle of achieving hybrid operational capabilities within NATO, due to the limited resources for the defence at Member State level.

---

[3] Laurenţiu Grigore, *Viitorul războiului – Războiul hibrid*, Buletinul Universităţii Naţionale de Apărare *"Carol I"*, no. 2, Editura Universităţii Naţionale de Apărare *"Carol I"*, 2015, p. 189.

[4] *Ibidem*.

IMPLICATIONS FOR THE FUTURE PHYSIOGNOMY OF LAND FORCES OPERATIONS

The operations of the land forces will be integrated into the JIM concept, which implies the existence of military capabilities that will be used in the full spectrum of military actions.

In this context, the land forces leadership must formulate the appropriate response options to the full range of risks and threats existing in the operational environment and institutionalize the typology and physiognomy of the military actions to be conducted at the national and multinational level.

Our opinion on the future land forces operations reveals the necessity of refining documents that orient and direct the activity towards the operationalization of those capabilities that will ensure the fulfilment of the established missions.

Based on these conceptual elements, we consider that the land forces must deal with the typology and physiognomy of the operations in which they will participate in the future, in correlation with the capabilities, goals, and allocated resources.

In our opinion, land forces must possess their flying capabilities (UAVs, attack helicopters, transportation helicopters), which are essential to improve information gathering capacity, manoeuvrability, and air-to-surface support.

For the participation of land forces in combat operations, we believe that it is necessary to achieve the appropriate capabilities to this range of missions gradually. For this, it is necessary the existence of certainties in the allocation of the necessary resources.

Secondly, based on the options formulated at the conceptual level, the land forces have to develop adequate capabilities (forces for special operations, CBRN, EOD, medical units) that can partake in the execution of unconventional operations, especially in the multinational context. If we include in the normative acts the participation of conventional units belonging to land forces in this type of missions, without designing and operationalizing specialized forces, the problem of successfully participating in the execution of some unconventional operations is not solved.

Thirdly, options that lead to the activation of conventional/unconventional capabilities to participate in the execution of missions in the irregular conflicts carried out in different theatres of operations have to be issued. This is a requirement at NATO level, but to what extent the participation of land forces in irregular actions will be ensured, will depend on the choice and vision of the political and military decision-makers.

Fourthly, we consider that it is of interest to achieve within the land forces some capabilities to counter cyber threats. It is well-known that this type of mission

is very sensitive and requires high-performance equipment and proper procedures. The last conflicts carried out recently included the cyber component, paralyzing the command and control systems, communications and computer equipment, and altered the dynamics and success of the operation.

CONCLUSIONS

This options regarding the physiognomy of the military actions in which the land forces will participate in the future express the need to direct the effort in order to achieve the adequate capabilities for performing hybrid operations.

In the present complicated context, the contemporary operational environment does not guarantee that complex crises and armed conflicts cannot be generated in different areas of the world.

This is why we consider that the military action has a cyclical nature, the sense of its evolution in the future being marked by the combination of the combat operations with unconventional, irregular operations or counteracting cyber threats. This reality requires the existence of adequate capabilities for the management of hybrid conflicts.

In this uncertain context, the military leadership must express a firm choice regarding the necessary capabilities well-suited to execute operations that ensure the promotion and defence of national interests, as well as the accomplishment of obligations within NATO.

The arguments presented synthetically above, determine us to promote the need to design, develop, and sustain a strategic vision. It must unequivocally express the option and level of ambition to achieve and operationalize those military capabilities that will ensure the engagement of the armed forces in hybrid operations, in both national and multinational contexts.

BIBLIOGRAPHY

1. ***, *Conflicte militare. Lecții învățate*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2010.
2. Laurenţiu Grigore, *Viitorul războiului – Războiul hibrid*, Buletinul Universităţii Naţionale de Apărare *"Carol I"*, no. 2, Editura Universităţii Naţionale de Apărare *"Carol I"*, 2015.
3. Ion Mituleţu, *Tendințe privind evoluția fizionomiei acțiunilor militare*, Scientific paper, *Tactică şi artă operativă – forţe terestre (TAOFT)* Scientific Conference, Bucureşti, 2014.

SYMMETRY AND ASYMMETRY IN RECENT MILITARY CONFLICTS

Florian RĂPAN, PhD

Professor, "Dimitrie Cantemir" Christian University, Bucharest

The changes that have taken place internally and internationally in the last decades in the political, economic and military field have led to contradictory and surprising evolutions. Of all the mentioned areas, the military one has perhaps suffered the most spectacular transformations, which have involved reorientations, re-evaluations and reorganisations in the system of planning and developing military actions. The so-called declarations of war have disappeared. Humanitarian reasons, the democratisation of the target state or the fight against terrorism are increasingly brought into the discussion. In some situations, international organisations are the ones that take the diplomatic initiative. The analysis of the unfolding of the military conflicts in the post-war period highlights the increased weight of the technical-scientific factor in determining the ratio of forces and implicitly in achieving the imbalance that leads to obvious asymmetric effects. All military conflicts, without exception, during this period, were influenced to a great extent by the technological ascendancy over the means of conducting military actions. The wars of the last decades are good examples in this regard. The article wants to emphasise the fact that, under the present conditions, the disproportionate war is not only a consequence but also a project of the states in conflict.

Keywords: symmetry, asymmetry, non-contact military conflict, hybrid warfare, kinetic actions.

INTRODUCTION

In the Explanatory Dictionary of the Romanian Language, it is shown that "*symmetry is the property of a spatial ensemble of being composed of mutually corresponding elements and of presenting, on this ground, certain regularities...*"[1]. In order to define and understand the concept of symmetry in the military context of the analysed issue, we can easily imagine that an "*ensemble*" in this respect can also be an armed conflict, and its main component elements will be the two parties involved in the conflict. Defining the concept of symmetry of armed conflicts in this way, with the help of the same dictionary, we can conclude that the asymmetry of conflicts can be nothing more than the *"lack of symmetry"* regarding the approached element.

We can state, at least theoretically, the existence or, from case to case, the non-existence of symmetry in some military conflicts. Thereby, we can speak of symmetrical and asymmetrical armed conflicts.

The recent period has been a testament to many conventional, symmetrical, asymmetrical local conflagrations, which instead of solving the problems that have arisen, have been disturbing the international relations, proving that the inter-state disagreements cannot be settled by the force of arms. There are several arguments in this regard, but the most relevant example is the Middle East, where major confrontations took place in the post-war period (1948-1949, 1956, 1967 and 1973), and the current situation in the area is so tense that a new major armed conflict between Israel and the Arab world could burst at any moment.

The mechanisms that trigger conflict situations polarise the interests of power centres. Their support for one side or another of the protagonists creates imbalances/asymmetries, paving the way for interference to obtain direct or camouflaged privileges, consolidating and widening dominant positions that may in fact be the real causes of major conflicts and their persistence over time.

The decisive domains of power are specified in a remarkable study of geopolitics. These would be: military, economic, technological and cultural. It is also mentioned that new dimensions of power can be added to them: communications, information, trade and finance.

Of course, all those are in close correlation to the geopolitical dimension[2].

[1] DEX, *Dicţionarul Explicativ al Limbii Române*, Editura Univers Enciclopedic, Bucureşti, 1998, p. 998.

[2] Zbigniew Brzezinski, *Marea tablă de şah,* Editura Univers Enciclopedic, 2010, pp. 12, 35.

Consequently, the power gap has triggered some military actions by which it was erroneously evaluated that an easy victory would be achieved by the purely mathematical effect of numerical and technical superiority as a result of the strategic asymmetry of forces and means.

Moreover, during the course of some of the conflicts triggered under such conditions, unforeseen situations have appeared which have substantially modified the initial data of the situation, producing changes and sometimes reversals of strategic asymmetry or, from case to case, the transformation of symmetry into asymmetry. Two major military conflicts are revealing in this regard, in which the USA and USSR were engaged, the main actors of the *Cold War*: the war in Vietnam (1964-1973) and the war in Afghanistan (1979-1989).

All military conflicts, without exception, carried out during this period were influenced to an overwhelming extent by the technological ascendant of the means of conducting combat actions. Arab-Israeli wars, the Falkland Islands conflict, the Gulf, Yugoslavia and Ukraine wars are significant examples.

TYPOLOGY OF ASYMMETRIC CONFLICTS

There are several classifications of conflicts and wars, depending on a multitude of criteria. Regarding the asymmetric strategies, it must be said that they are related to the nature of the conflicts and the way they are developing, the exit from linearity and the entry into the multidimensional space. The war is anchored in the reality of each era and the reality of the 21st century is informational, spatial, fluid and asymmetrical. Today, the world is very different. Worldwide there are too many gaps to provide optimal conditions for the development of any symmetry.

The strategy, no matter how modern derivative, is inseparable from the notion of conflict, and the latter is inconceivable without the friendly-enemy correlation. Therefore, the strategy is about the conflict area and this area includes, first of all, the war, as an extreme form of conflict. In this regard, we can see that the war, as an armed conflict, with two or more belligerents, passes through the following phases:

- the ancient war of invasion, triggered by surprise, with specialised armed forces, which was an asymmetrical war, since the warring nations attacked sedentary people, initially unarmed and unprepared for such confrontations;
- the classic war, characterised by the confrontation, most often within the limits of the law of peace and war, between two armies approximately equal in training, endowment and strategy (Napoleonic type wars, the First and the Second World War). These were symmetrical wars;
- the modern war, which has a lot of forms and manifestations, from the classical, generally symmetrical ones, to the non-contact ones, which are

obviously asymmetrical[3], from those of sanctioning or imposing a certain behaviour to the terrorist ones;
- the violent conflict which in turn includes armed conflict other than the war with the belligerents and the non-armed violent conflict.

One of the most important elements of the confrontation asymmetry is given by **space**. Its fundamental feature in modern warfare is fluidity. *"The fluid combat space is a surface of land determined by the maximum possibilities of the large units or units to discover and engage the enemy simultaneously at all three levels of military art (tactical, operational, strategic) in at least two environments simultaneously for the purpose of decisive blow of the centres of gravity/its decisive points and its psychic and physical defeat"*[4].

Several types of asymmetrical military conflicts are known in the specialised literature, namely: non-contact war, disproportionate war, people's war (total), guerrilla war, armed revolution, civil war and terrorism. Lately, hybrid warfare has been included by some military analysts in this category, although there is no unanimous acceptance in this regard.

Non-contact warfare is an effect of new technologies. However, his causality lies elsewhere. New technologies have the ability to prevent direct contact, which has always been destructive and has produced numerous human victims. To this end, a wide range of means have been used, from the informational ones to the ones of misinformation and misleading, from the strategic manoeuvre to the blow with the help of strategic missiles and aviation.

Certain aspects of non-contact actions (at least in terms of their preparation and deployment stages) have been shown at almost all times in almost all wars and military strategies.

The problem of non-contact warfare has been marked by the dramatic experience of the Americans in Vietnam.

It is interesting that the new type of non-contact war is not due to the intrinsic revolution of military art but to the pressure of civil society, specifically American society, which no longer accepts (at least after the terrorist attack of September 11, 2001) human sacrifices in conflict areas, no matter what the goals and objectives of the war. Today, American society – a super-technologised one – no longer agrees to human losses, at most it can accept certain expenses.

The non-contact war, theoretically, was born, in a way, from the strategic concept *Air Force Battle – 2000* and from what at that time was called the *Deep Shot*. This concept represents only a modernisation of the classic concept of warfare, that is a wide air manoeuvre allowed by the modernised means (weapon systems) that were beginning to enter the armed forces of NATO member countries.

[3] T. V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers,* Cambridge University Press, 1994.
[4] Gl. bg. dr. Paul Vasile, *Războiul mileniului trei,* Editura D.B.H., București, 2000, p. 102.

The 1991 Gulf War against Saddam Hussein's army was the first modern, successful formulation of this type of war.

Asymmetry, in non-contact warfare, is still relative, difficult to evaluate and predict. It is, as a rule, an expression of a disproportionate reality, but it does not necessarily mean disproportion, inferiority or superiority but only a difference in terms of the forces, doctrines, concepts and means used, mentality and strategy. Non-contact warfare is becoming more and more an operational reality of the present and is expected to be an important feature of the future. However, non-contact war does not necessarily mean asymmetry, meaning a difference (differentiation of the parts separated by an axis). It means only actions at a long distance, apart from a *stricto sensu* contact in which different or approximately equal forces may be confronted by different strategies or similar strategies.

Disproportionate warfare is entirely a product of asymmetrical strategies. But, in turn, it produces asymmetrical strategies. Disproportionate warfare is a concept, but it is also a fact. Like asymmetric strategies, it results from a reality-based on disproportions. In a world where the chances are different, the confrontations are different too. Differences and disproportions are also a reality, a goal and a means of promoting policies and materialising the interests of the states.

The latest military clashes in Iraq, former Yugoslavia and Afghanistan are nothing more than current forms of the disproportionate war. Moreover, the imposition of certain interests or behaviour is of a disproportionate nature. Specifically, there are disproportionate non-contact wars.

This concept is not new. In one form or another, we encounter it in all kinds of military confrontations and expresses itself in what is commonly called a force report. We can consider the disproportionate war as a solution to forcefully resolve a dispute as a rule for the imposition of a certain type of behaviour, the belligerents being *ab initio* in major disproportionality in terms of the political point of view, forces, means and the adopted strategy. On the one side, there is a great power, a strong military alliance or a group of states, and on the other side there is a *"rebel state"*, a dictatorial regime, a centre of the proliferation of violence, terrorism, instability or other threats.

Another example of disproportionate war is the one that is currently taking place between Israel and the Palestinians. Israel acts or reacts with well-organised armed forces and powerful means of combat, while the Palestinians act or react through what they call the *Intifada*, the total war, the holy war, which is nothing more than a form of guerrilla warfare and terrorism or all forms of action and reactions in one place.

In consequence, the disproportionate war appears in the following situations:

- as the last means for the imposition by force of a state or a population, of a certain type of behaviour, dictated or decided by the interests of a great power of a coalition of states, an alliance or the international community;
- as the last means of imposing peace;

- as the last way for the removal of forces from outside of a dictatorial regime;
- as a way of liquidating the resistances that oppose the establishment of the new world order;
- as a way of revenge especially through terrorism and other unconventional actions.

The conditions under which such a war is waged are as follows:

- crushing political will;
- indisputable technological superiority;
- coalition of states to achieve a grouping of forces impossible to equate (e.g. the coalition of states against Iraq or against Libya in 2011);
- UNO mandate;
- the existence or triggering of general hostility against the target state (of the region, area, population etc.).

The reactions of the state (region, area, population etc.) targeted by such a war can be very different: from immediate submission to response actions (usually by guerrilla or terrorism) or to total war.

Such a war aims to paralyse the reaction, in the first place. Therefore, it is evolving in all the environments and through all means. The blow is also political, media, informational on the command and control systems, on the economy (embargo), culture, education and, of course, on the armed forces. Such wars tend to become (at least in NATO's strategic concepts) a way for Western democracies to enforce human rights, to eliminate dictatorial regimes, to prevent and discourage crises, to combat terrorism, to secure or impose peace.

The People's War (total). It appeared as a reaction to the disproportionate war. Such a war usually leads to technological inferiority and consists of the total mobilisation of resources (demographic, moral, material, cultural, territorial) to deal with an invasion. At least that's how it was defined over time. This type of war is one of the most conclusive expressions of asymmetrical strategies. The power of technology opposes the will of an entire people to preserve their country, language, traditions, way of life. Such an objective of war seems generous and heroic. The popular type of war is specific to the epoch of nations. The wars of national liberation largely took the form of the people's wars (China, Yugoslavia). In some countries, however, they turned into clan wars for the seizure of political power and led to the destruction of the respective countries (Somalia, Angola, Algeria).

Therefore, in the modern era, in the present and especially in the future, it seems that total wars lose their importance because of, on the one hand, the process of globalisation (which is directed against the individuality and supremacy of nations) and, on the other hand, the improvement of the means of combat, the professionalisation of the armed forces and the emergence of non-contact wars.

This type of war has left Iraq, Lebanon and especially Yugoslavia in the impossibility to have a proper reaction.

In other words, in the age of informational societies, total war – as we know it – seems no longer possible, because no country in the world can be willing to accept being hit from a distance. That is to expose its population, economy, territory and values accumulated over the centuries to blows that it can neither counteract nor stop.

While the total war seems no longer possible, the guerrilla loses nothing of its traditional force.

Guerrilla is a product of the asymmetrical strategy and consists of an unconventional response, through violence, to an unconventional policy generally carried out by states but also against states. Guerrilla fighters act according to the rules of the attacks by surprise, harassment, destruction and even by means of terrorism. Guerrilla strikes both weaknesses and strengths, seeks vulnerabilities, sensitivities, but also key points and centres of power.

Guerrilla actions have no logic, no morals, no rhythm, no rules. They take place day and night, everywhere and by all means. Guerrilla fighters act in small groups with light weapons, according to the rules of the armed fight, conspiracy and even terrorism. Therefore, the guerrilla is very difficult to control and counter. After the Second World War, this way of fighting took on an unprecedented development, especially in Latin America but also in Africa, Asia, the Caucasus and even the Balkans. It should be noted that in almost all situations[5] the actions of the guerrillas achieved their intended goals or at least some of them.

Guerrilla was fought especially against the governments of certain countries, taking the form of violent armed actions, developed by surprise, pursuing separatist goals, claiming objectives, some aimed at gaining political power, others at the collapse of national states or obtaining financial, material or territorial advantages.

Guerrilla warfare – as an asymmetrical form of action or reaction – is considered uncomfortable and very dangerous no matter the opposing forces and means. Colombian guerrillas, Albanian ones from Kosovo and Macedonia, ETA and IRA, as well as Afghan and Chechen ones, were a major problem for the state authorities and international organisations trying to control or at least to contain the phenomenon.

Although it also uses the means and methods of terrorism, the guerrilla is not terrorism. Guerrilla is a war that is subject to a single theory – chaos – but not to the whole theory. Guerrilla is a war of situations, not a war situation.

[5] The actions of the Kosovo Liberation Army led to the creation of an extremely complex situation, which required the intervention of the UNO, then NATO, taking away Yugoslavia's right to control the province and placing it under international control; likewise, the action of the Liberation Army from F.R.I. Macedonia determined NATO intervention and reached an agreement that was intended to favour the Albanians in F.R.I. Macedonia.

The armed revolution. The term revolution is widely used and highly controversial. By this term, everyone understands a way to change one order after another, that is a way of processing power through violence. The revolutions so far – starting with the French one in 1789, continuing with the Bolshevik one in 1917 and ending with the Romanian one in 1989 or with the Arab primordial revolutions of the year 2010 – have done nothing else but to change one regime with another and replace the ruling power with another one in the name of principles, more precisely, of some interests.

Revolutions, including the armed ones, are political. The revolution is a rapid action often triggered by surprise, which includes masses of peaceful manifestations and violent outbursts through which the takeover of power and the implementation of a reform program based on other principles and in relation to another perspective can follow. Revolutions are the result of some accumulations, they are great outbursts of energy, ways of radical social change, real changes and changes to a new human situation, they are genuine asymmetrical conflicts.

Civil war is that type of war that results either from the failure of a revolution (and then it carries, at least in the initial stage, the mark of asymmetrical strategy) or from the struggle for power between groups of internal forces, being its last stage, the armed, violent one.

The main feature of the civil war is that it takes place within a country, between two or more forces seeking to gain political power. Under these conditions, civil war should belong to symmetrical strategies, with each party having goals and even the same means to achieve them.

However, civil war is part of the spectrum of asymmetrical strategies due to the very large, often unpredictable, range of actions. The civil war can also be called the one in Bosnia since 1995, by the Bosnian forces and the army of Bosnian Serbs. Only, in the end, this war, like most wars in the former Yugoslavia, started to look like a classic confrontation between two regular armies. The same thing happened with the wars in Somalia, Angola, Northern Ireland and, in a way, with those in the Caucasian area, which evolved between asymmetrical strategies (in the sense of the involvement of the great powers and international organisations) and strategies of symmetrical confrontations.

Terrorism is considered, after ethnic conflicts[6], to be one of the biggest threats to security and stability. Organised crime and terrorism have proliferated in the past few decades so that, at the beginning of the third millennium, there is almost no state or international organisation that is not interested in the problem of defence and protection against this scourge.

[6] Joseph Yacoub, *Minorités nationales et prolifération étatique*, in *La Revue Internationale et Stratégique*, no. 37/2000.

Terrorism is both an aggression and a reaction to aggression. As aggression, it aims to create an unstable situation of fear and terror that will benefit certain circles. This notion – certain circles – is hardly identifiable and equally difficult to quantify.

However, there is another kind of terrorism, which presents itself as a reaction of the weak to the powerful. In this sense, terrorism presents itself as an expression of disproportionate war, as a reaction to this type of war. International law does not accept it, the great powers repress it, international bodies condemn it. But it exists and continues to grow.

The forms of manifestation of terrorism are very diversified and, for this reason, terrorism has no limits. Terrorism seen at planetary scale represents a true war – the millennium war carried through all possible means.

THE HYBRID WAR BETWEEN CONVENTIONAL AND UNCONVENTIONAL ACTIONS

The concept of *hybrid warfare* emerged and was developed by US military specialists over the last decade, to emphasise the need for permanent adaptation of US military forces to the realities of the modern operational environment. The initiators of the development of the concept were a group from the US Marine Corps, led by James Mattis and Frank Hoffman[7]. In 2005, the two published the article *"Future Armed Confrontations. The Emergence of Hybrid Wars"*[8], in which it was shown that the wars in Afghanistan and Iraq influenced the process of balancing American strategic thinking, which was then considering viable ways of responding to a broad range of threats to USA interests. However, it was emphasised that the conventional threat will never go away, and the US military must maintain its superiority in this area, in order to be ready to wage a major, high-intensity war at any time[9].

American military doctrine specifies that the US army recognises two basic forms of war – *traditional* and *irregular*. Further, it is specified that the element that delimits the two forms of war is the *strategic focal point* of each of them. In other words, the war is traditional or irregular depending on the strategic purpose pursued by each of the two forms. To this assertion, we can mention that,

[7] The concept of *"hybrid warfare"* came about in 2005. Lieutenant Colonel (ret.) Frank G. Hoffman was working at the Center for Threats and Opportunities, Quantico – Virginia, along with Lieutenant General James N. Mattis, who was the commander of the Combat Preparation Command to the US Marine Corps.

[8] Frank G. Hoffman, James N. Mattis, *Future Warfare: The Rise of Hybrid Wars*, in *Proceedings Magazine*, vol. 132/II/1,233, US Naval Institute, November 2005, available at http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf, retrieved on 11.08.2019.

[9] Valerică Cruceru, *"Despre conceptul de război hibrid în gândirea militară americană",* in *Buletinul UNAp*, September 2014.

next to the purpose, important elements that confer the character and finally the type of war are the means by which the war, the structure and missions of the forces involved in the conflict, as well as the set of *tactics, techniques and procedures/TTP*[10] used to carry out the actions.

Returning to the doctrine, this specifies that, from a typology point of view, there is a duality, involving both dimensions, traditional and non-traditional, in both forms of combat: offensive or defensive.

The book *"Hybrid War: A New Paradigm for Stability Operations in Failing States"* published by Margaret S. Bond, in 2007, develops a different strategic notion that describes the means of using the USA armed forces in hostile fighting environments attributed to conflict-affected states. The support actions in which the military forces participate lead to a considerable increase in efficiency and must be carried out at the level of each instrument of national power. By taking such actions at the political, diplomatic, economic and informational level, achieving the political objectives in relation to the military ones is much more realistic. Margaret S. Bond believes that: *"in the future, the war will be hybrid and will include all elements of national power, applied successively and uninterruptedly in support of stability, security and reconstruction operations and, last but not least, the armed struggle"*[11].

In this context, hybrid warfare can easily resort to non-lethal tactics and procedures, but it can also stage lethal means. All military, economic, informational, diplomatic and political activities are intertwined to amplify the persuasive effects of the hybrid war.

Therefore, hybrid warfare comprises both the elements of conventional warfare and the elements of unconventional warfare. The confrontation of the doctrinal elements of the conventional war with the characteristics of the unconventional war results in the hybrid war, thus causing strategists to ask themselves what the physiognomy of the future wars will be.

Although hybrid warfare highlights the complexity of warfare, its components are not new war elements.

The hybrid character of recent conflicts determined Anders Fogh Rasmussen, General Secretary of NATO during 2009-2014, to declare at the Summit in Wales that hybrid war represented *"a sophisticated combination of traditional conventional warfare mixed up with information and primarily misinformation operations"*[12].

[10] ***, AAP-15, *NATO Glossary of Abbreviations Used in NATO Documents and Publications*, NATO Standardization Agency, 2013.

[11] Margaret S. Bond, *Hybrid War: A New Paradigm for Stability Operations in Failing States*, US Army War College, Carlisle Barracks, Pennsylvania, 2007, p. 4.

[12] Ian Traynor, *Ukraine Crises: NATO Plans East European Bases to Counter Russia. NATO Chief Announces Move in Response to Ukraine Crises and Says Alliance Is Dealing with a New Russian Military Approach*, in *The Guardian*, August 2014, http://www.theguardian.com/word/2014/aug/26/nato-east-european-bases-counter-russian-threat, retrieved on 03.09.2019.

Addressing the concept of *"hybrid war"* in the Declaration of the NATO Summit in Wales outlines the path of the specialised themes based on the hybrid war and their transfer from the research phase to the NATO application area.

The statement of the NATO Summit in Wales recalls the need to take measures and elements that will not prevent the Alliance from being able to *"effectively address the specific challenges posed by hybrid warfare, where a wide range of overt and covert military, paramilitary and civilian measures are employed in a highly integrated design"*[13].

This statement recounts the American authors' definitions of hybrid warfare. Both NATO, on the whole, and the members of the Alliance, individually, by accepting the content of the declaration, are adopting in this way the American perspective on hybrid warfare, despite the fact that it does not have a unanimously accepted definition within the US Department of Defense.

The same statement stipulates the need for increasing the capacity of NATO member states and for possessing *"the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats and the capabilities to reinforce national forces"*[14].

This new concept of warfare has become fashionable among the political and military leaders, as well as in the civilian environment. However, Clausewitz wrote almost two centuries ago that although war changed its characteristics in various circumstances, war was still war. The war of the 21st century has been a rather complex phenomenon, but in essence it has not changed and will not do so. By carefully examining history, this new concept of hybrid warfare is a useful means of thinking and understanding the past, the present and the future. However, the war horizons of the 21st century are becoming increasingly uncertain. The security challenges of the great powers include inter-state wars, the fight against insurgents, terrorism, and combinations thereof.

At the moment, the conventional military supremacy of the great powers will force the potential enemies to develop alternative means in the near future to oppose the conventional state power. More and more international actors will include these means as well as irregular or hybrid forces working in tandem. Potential enemies will try to combine different approaches to war to meet their strategic doctrine and culture, the geographic reality but also the economic one. Against these opponents, technological superiority is useful, but not always sufficient. As it has been demonstrated in the wars in Iraq and Afghanistan, it is necessary to turn victories from the battlefield into long-term strategic gains.

[13] *Wales Summit Declaration*, issued by the Head of State and Government participating in the meeting of the North Atlantic Council in Wales, September 2014, pct. 13, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease, retrieved on 03.09.2019.

[14] *Ibid*.

On the other hand, the history and culture of the adversaries must be understood and specially trained troops must be used in order to prepare the population on how to deal with social violence.

The hybrid war will be a critical challenge for the great actors of the 21st century, a challenge openly acknowledged by the great powers. In order to counteract their potential hybrid opponents, the big players on the geopolitical scene must understand the hybrid war as well as possible.

Hybrid opponents use combined combat capabilities in order to gain an asymmetrical advantage. An example of this type of hybrid action is found in 2006, in the operation of the Palestinian organisation Hezbollah in conflict with the Israeli armed forces. Hezbollah's armed wing used at that time a combination of conventional military actions (the use of classic fighting forms) and hybrid military actions (combat forces dressed in civilian clothing, using the population as a human defence shield).

Hybrid warfare is defined as a combination of conventional, unconventional and asymmetrical means, including continuous handling of political and ideological conflicts, and may contain a combination of special operations and conventional military forces, intelligence agents, political provoking agents, media representatives, acts of economic intimidation, cyber-attacks, paramilitary forces, terrorist forces and criminal elements[15].

The hybrid war involves actions carried out on several levels, meant to destabilise the functioning of the state body, disorient and manipulate the population of the target state.

Thus, potential adversaries such as groups of states, states, hostile religious ethnic groups have access to modern military capabilities, including command and control systems, rocket systems, cyberwar systems, which in combination with the use of insurgent fighting methods – ambush, use of improvised explosive devices (DEI), kidnappings and assassinations, provide them with an advantage over military forces carrying out conventional actions.

In this context, we cannot exclude the possibility of the emergence of vectors that have means of attack in the information spectrum (cyberwar), through which to trigger cyber attacks with catastrophic social, economic and/or military results for the target states.

The study of the main forms and methods of hybrid warfare is based on comparison with conventional warfare forms and methods, as follows:

- declaration of war vs. undeclared war;
- military actions vs. subversive attacks;

[15] Robert A. Newson, *Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There?* in *Janine Davidson Blogspot: Defense in Depth*, 23 October 2014, http://blogs.cfr.org/davidson/2014/10/23/, retrieved on 02.08.2019.

- coercive diplomacy vs. economic blackmail;
- conventional means of combat and regular military forces vs. fighting means and unconventional forces.

The dynamics of the events that have taken place in the global security environment unfolds at an intense rhythm, and the diversified type of military actions, with spontaneous and sometimes unnoticeable crossings, from the conventional to the unconventional, and vice versa, reinforces the idea of approaching the state of conflict as a part of hybrid warfare.

Analysing the current conflicts, characterised as hybrids, we find that they do not resemble each other. In hybrid conflicts, the tactics and methods used differ from one area to another, from one actor to another, depending on the security situation and the geopolitical context. When the ISIS terrorist organisation has made its way, using violent means and using terrorism to western Iraq, observers described this type of confrontation as a *hybrid war*. In the same way, there have been evaluated the actions of the rebels from Ukraine who took control over the industrial regions of the southeast of the country.

The actions taken to annex the province of Crimea and subsequently the actions of the Russian Federation in the Donetsk and Luhansk areas of Eastern Ukraine are considered by the community of Western states as a model or pattern of aggressive action from Russia, applicable to all states in the former Soviet area. The actions of the Russian Federation in Crimea were carried out in the form of undercover military operations that combined ambiguity, misinformation and element of surprise at an operational level with conventional military actions and actions specific to electronic and informational warfare.

The annexation of Crimea ended with the use of Russian military forces stationed on the peninsula to occupy and take control of the main military, economic and administrative objectives.

The initial hybrid actions of the Russian Federation in Eastern Crimea include the taking and assault of the Crimean Peninsula Parliament by the Russian special forces. This was accompanied by other actions specific to the hybrid war such as:

- invasion of the peninsula by Russian armed units whose fighters did not wear military insignia;
- blocking the Ukrainian ports and vessels of the Ukrainian navy by the Russian Black Sea fleet;
- organising, arming and coordinating by Russian military instructors of Russian ethnic locals for the formation of a 5th Column among the population;
- encouraging the establishment of an Executive Authority of the Crimean Peninsula, which organised a referendum for annexation to the Russian Federation under the influence of the Russian occupation forces;

- signing an agreement by which, following the referendum, the self-proclaimed Supreme Radar of the Autonomous Republic requested to join the Russian Federation;
- conducting propagandistic actions to influence the western public opinion, materialised by numerous declarations and pressures in the diplomacy and in the media.

A particular feature of the hybrid actions carried out by the Russian forces that contributed to the success of the operations in Crimea is the existence of the agreements of transit of the Ukrainean territory by the Russian military forces. Thus, by the deliberate violation of the provisions of these agreements, the Russian military forces infiltrated the national territory of Ukraine, under the pretext of carrying out military exercises.

Another feature of Russian actions in Crimea is the influence of public opinion and the population of the Crimean Peninsula through the use of mass media and propaganda. Recent studies[16] have found that 84% of Russian and Ukrainian ethnicities in Crimea became supportive of the annexation, following Russian propaganda through the media, by inoculating the perception that ethnic Russians could become second-class citizens in Ukraine[17]. Another conclusion of these studies, which shows the effectiveness of the Russian media, is that, unlike the inhabitants of western and central Ukraine, a large majority (85%) of the population of the Crimean peninsula is not perceived as European.

Following the annexation, Ukraine has not acted in the information space that is broadcast in Russian, thus the Russian media has created a dominant and favourable position for transmitting and adapting information in support of the Kremlin's objectives[18].

Thus, the actions carried out by the Russian Federation for the purpose of annexing the Crimean Peninsula were within the range of hybrid actions, without implying the development of conventional military actions, reaching the proposed goals.

In this context, the most important question for the Romanian political-military decision-makers will not be, essentially, the matrix of the hybrid war, but rather the mode of action of a great power, such as the Russian Federation, or the mode of action of international terrorist organisations, in the case of employing the entire range of hybrid actions, in order to achieve the set goals. The answer to this

[16] John O'Loughlin, Gerard Toal, *Mistrust about Political Motives in Contested Ukraine*, in *Washington Post,* 13 February 2015, available at http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/02/13/mistrust-about-political-motives-in-contested-ukraine/, retrieved on 05.08.2019.

[17] Johnson's Russia List (blog), *The Crimean Conundrum*, 6 March 2015, available at http://russialist.org/the-crimean-conundrum/, retrieved on 05.08.2019.

[18] Michael Kofman, Matthew Rojansky, *A Closer Look at Russia's Hybrid War*, in *Kennan Cable*, no. 7, April 2015, p. 5.

question should reflect how Romania, as a member and strategic partner of the North Atlantic Treaty Organization, identifies and designs defence measures against threats and hybrid actions.

CONCLUSIONS

In support of these statements, statistics show that, in about 90% of the wars during the post-war period, the initiator of the armed conflict did not obtain a victory that would ensure the full achievement of the proposed purpose. In 44% of cases, the political configuration in the conflict area did not change as a result of the resort to armed violence, and in 55% the conflict situation was further complicated. In history, there have been wars that have achieved their goals and objectives and others that have not. The condition of success, superiority in the armed forces was in regular cases decisive. Currently, this rule is no longer fully valid, the promotion of major political interests through the armed forces is increasingly restricted. As a consequence, the responsible political factors seek other ways and other means, especially non-violent ones, to achieve their goals.

Despite the international efforts that are being made to resolve peacefully the differences and crises that arise between states or groups of states, however, there are forces that support the violent way of solving them as the only effective means in this direction. Thus, the power gap has, over time, been the most important element that allowed powerful states to impose their will at the expense of the weakest.

The analysis of the recent conflicts unfolding highlights the increasing weight of the technical-scientific factor in determining the ratio of forces and implicitly in achieving the imbalance that leads to notable asymmetric effects.

Recent events in the current security environment highlight the fact that new conflicts present different forms of violence. Starting from terrorism, organised crime, insurgent actions, intimidation movements and attacks in cyberspace, the simultaneous use of at least two of them leads to major social effects.

International security will continue to face a series of regional, transnational, asymmetrical dangers. As a whole, all these dangers, either smaller or greater ones, represent a major obstacle to globalisation and will continue to absorb much of the armed forces' time, energy and resources.

BIBLIOGRAPHY

1. ***, AAP-15, *NATO Glossary of Abbreviations Used in NATO Documents and Publications,* NATO Standardization Agency, 2013.
2. DEX, *Dicţionarul Explicativ al Limbii Române*, Editura Univers Enciclopedic, București, 1998, p. 998.
3. *Wales Summit Declaration*, issued by the Head of State and Government participating in the meeting of the North Atlantic Council in Wales, September 2014, pct. 13, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease, retrieved on 03.09.2019.
4. Johnson's Russia List (blog), *The Crimean Conundrum*, 6 March 2015, http://russialist.org/the-crimean-conundrum/, retrieved on 05.08.2019.
5. Margaret S. Bond, *Hybrid War: A New Paradigm for Stability Operations in Failing States*, US Army War College, Carlisle Barracks, Pennsylvania, 2007, p. 4.
6. Zbigniew Brzezinski, *Marea tablă de şah,* Editura Univers Enciclopedic, 2010.
7. Valerică Cruceru, *Despre conceptul de război hibrid în gândirea militară americană*, Buletinul UNAp, September 2014.
8. Frank G. Hoffman, James N. Mattis, *Future Warfare: The Rise of Hybrid Wars*, in *Proceedings Magazine*, vol. 132/II/1,233, US Naval Institute, November 2005, available at http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf, retrieved on 11.08.2019.
9. Michael Kofman, Matthew Rojansky, *A Closer Look at Russia's Hybrid War*, in *Kennan Cable*, no. 7, April 2015, p. 5.
10. Robert A. Newson, *Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There?* in *Janine Davidson Blogspot: Defense in Depth*, 23 October 2014, available at http://blogs.cfr.org/davidson/2014/10/23/, retrieved on 02.08.2019.
11. John O'Loughlin, Gerard Toal, *Mistrust About Political Motives in Contested Ukraine*, in *Washington Post,* 13 February 2015, available at http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/02/13/mistrust-about-political-motives-in-contested-ukraine/, retrieved on 05.08.2019.
12. T. V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers,* Cambridge University Press, 1994.
13. Ian Traynor, *Ukraine Crises: NATO Plans East European Bases to Counter Russia. NATO Chief Announces Move in Response to Ukraine Crises and Says Alliance Is Dealing with a New Russian Military Approach*, in *The Guardian*, August 2014, http://www.theguardian.com/word/2014/aug/26/nato-east-european-bases-counter-russian-threat. retrieved on 03.09.2019.
14. General de brigadă dr. Paul Vasile, *Războiul mileniului trei,* Editura D.B.H., București, 2000, p. 102.
15. Joseph Yacoub, *Minorités nationales et prolifération étatique*, in *La Revue Internationale et Stratégique*, nr. 37/2000.

FORMALISING INFORMATION WARFARE

Alin-George IONESCU

"Samoilă Mârza" Centre for Psychological Operations, Bucharest

Is Information Warfare a modern-day reality or just a theme for theoretical and abstract debate? The evolution of humankind into the information society generated the premises for the development of methods specific to Information Warfare based on the advance of information technology in all domains. Super-powers included information-related aspects of warfare in documents that govern their national security. The following paper offers a theoretical approach to this subject. While it highlights the lack of doctrinal references and conceptualisation, it also gives a possible representation of the way state actors and organisations can act under the auspices of Information Warfare and briefly evaluates the potential objectives involved by the steps taken towards action.

Keywords: information warfare, operations, information society, deployability, media warfare.

INTRODUCTION – THE TRANSITION OF HUMAN SOCIETY TOWARDS THE INFORMATION AGE

The global information environment has undergone significant changes in the last decades and has experienced the emergence of new digital vectors and the decrease in conventional ones, produced in particular as a result of the radical changes brought about by the advancement of information technology.

The transition from an industrial society to an informational one started, according to American futurist John Naisbitt, with the launch of the Sputnik satellite, in 1957, by the Soviet Union (coincidentally or not, bearing the name of an important instrument employed in the information warfare currently carried out by the Russian Federation), which did not revolutionise the exploration of the cosmic space, as it was believed at that time, but the way in which humanity began to communicate through telecommunication networks.

This international interconnectivity has intensified by increasing the pace with which new technologies have been developed, which has had a direct impact on the speed of information spread, processing and storage, on the one hand, and the dramatic decrease in production costs of equipment and systems which provide these parameters, on the other hand.

The most important milestones in the transition to the information society are considered to be[1]:

- its representation as an economic reality, not as one that belongs to the intellectual abstract level;
- the innovation in the communication system and information technology that will accelerate the pace of change, removing the information privilege (the amount of time required for information to cross the channel between transmitter and receiver);
- information technologies that will be applied initially to the old industrial activities, and subsequently will generate new activities, processes and products;
- the new society, which will require intensive training and the educational system, which will always offer a weaker product.

[1] John Naisbitt, *Megatendințe*, Editura Politică, 1989, p. 50.

Here we could add two other aspects that are relevant to our approach:

- the information has acquired another value of use, besides the one that derives from the original meaning of the information technology, one from the perspective of the new dimensions of the human needs to be informed, to send and generate information;
- in the new society, a new industry or field of human activity has been developed in which information represents the raw material, for the first time an inexhaustible one.

The advances made by information technology have affected the global power balance, given that they have favoured the process of globalisation, increasing international interdependence, expanding the market economy, investment, and access to power of democratic forces to the detriment of totalitarian regimes whose main feature in this area was government control over society, including the information environment.

The way in which the new technologies in the field are used by the state or non-state actors is different and, even more, it may be difficult to predict, because of different political and cultural systems.

Certainly, the rapid evolution of the information society has favoured the United States in several ways, as expected, as the technology itself was expensive then, projecting it as an undisputed leader of a unipolar world, especially after the collapse of the Soviet Union.

From the economic point of view, an entire industry of information technology has been developed, as well as a great variety of replications in all fields of activity of humanity, mainly in the form of software applications, reaching today an absolute penetration of the new technologies in all domains of human activity.

In the military field, the United States has developed and implemented infrastructure elements related to information technology in the form of global high-speed data networks, which has led to significant progress in assigning military power by increasing the degree of deployment of forces, shortening the decision-making time and not least by enabling the ability to remotely command and control the battlefield from far distance. In addition to integrating the new technologies with the conventional military techniques to increase the strike precision, perform rapid calculations, develop applications that support the planning processes for decision-making, at the same time, in several states within NATO, concepts and doctrines for non-lethal domains have been developed and adapted, employing information from the point of view of the effects it can achieve on human receptors. Thus the psychological and information operations, generally regarded as part of the military actions, have become more widespread, as the new technologies have become accessible to the global population, which has allowed

the information to travel very quickly and be available to a growing number of people. Another important feature of the information society is the dissemination of information in an uncensored manner, which happens as a result of the exponential growth of information sources reaching the level where it can be considered that every internet user becomes a source of information. In this framework, the shift to the concept of using information as a weapon in a different way from that of the intelligence field was made.

THEORETICAL APPROACH

Stories about actions specific to the information warfare were published, for the general public, for the first time during the war in the former Yugoslavia, but the headlines really aroused the attention of both the global public opinion and the military specialists especially in the period that followed the annexation of Crimea in 2014 by the Russian Federation. However, it should be noted that this is not an element of novelty, at least from the point of view of limited practical approaches, even the World War II started with a disinformation in the media – *the Gliwice incident*, the element of novelty rather being represented by the scale of the actions and the wakefulness related to implementation of specific activities for information warfare at the state level. Considering that, at least statistically, in the case of other important conflicts of the last century, there were no elements assigned to make a direct reference to the information warfare, we can consider that a decisive factor that has contributed to the development and application of the concept is related to the information society and the expansion of the global computer network (through the emergence of the Internet) while dramatically reducing the cost of accessing it.

There has not been identified a recognised definition of the information warfare with a character of novelty, in specialised materials or official documents of the Russian Federation, in the publication of the *United States Department of Defense Dictionary of Military and Associated Terms 2019*, or in *AAP-6 NATO Glossary of Terms and Definitions, Edition 2018*. A term that is associated with the information warfare is represented by information aggression, which already has a definition in circulation being described as the illegal but especially immoral use of informational products (newsletters, TV shows, press articles) for malicious purposes, to manipulate, misinform or generate reactions within a target audience or organisation[2]. The use of the latter seems to be facilitated by the fact that it does not contain the term of *warfare* which in turn refers to an official declaration made by a state and also has a military connotation. However, this can easily

[2] Vasile-Dumitru Ionițoiu, Mihai Videscu, *Contrainformații în epoca post-adevăr*, in *Revista Infosfera*, no. 1, București, 2018, www.mapn.ro/publicatii_militare/arhiva_infosfera/index.php, retrieved on 17.07.2019.

be contradicted by the widespread use of expressions such as "*economic war"* or "*media war"* and which do not imply the official declaration of war between states. What differentiates these two terms from the information warfare is that they cover military issues to a very small extent, while the informational one can approach military aspects in a consistent proportion. On the other hand, the use of the term *information aggression* conveys a negative connotation, that leads ultimately even to physical aspects, which is not always the case when we use the term warfare.

The term *information warfare* was formally associated in the United States in the '90s with that of information operations. It was defined as "*information operations carried out during times of crisis or conflict (including war) for the purpose of obtaining or promoting the specific objectives of a particular adversary or adversaries"* while information operations used to represent "*actions undertaken to affect the information promoted by adversary and its information system at the same time as protecting their own information and systems*"[3]. These provisions were eliminated from the subsequent updates of the doctrine for information operations, a possible explanation being that, in the acceptance of joint operations, the information warfare can be considered only in the crisis and conflict phases, whereas the application of it in the peacetime was assessed to exceed the document purpose.

The information environment is the battlefield of information warfare, being represented by the information itself and the full spectrum of individuals, organisations and systems that collect, process and disseminate information. In this context, the information environment can be considered as part of the battlefield in the general understanding, as it is the case in crisis or conflict, or it may constitute itself a stand-alone battlefield if the information warfare is conducted as a sole direction for all actions, and here we can exemplify with the peace phase.

The approach to operations in the information warfare involves the dissemination of information, in very large quantity and diversity, which takes certain forms (text, audio, audio-visual, visual, signal) and are also relevant for the target audiences, characterised by a large number of individuals, through vectors that operate in the information environment.

FORMALISING INFORMATION WARFARE

Similar to the information society that needs to be understood and perceived as a reality today, the information warfare represents an ongoing process and must be approached as such, overcoming the barrier of abstract theoretical approaches. At the international level, aspects related to its development are taken into account

3 ***, *Joint Doctrine for Information Operations*, 1998, p. 13, www.c4i.org, retrieved on 15.07.2019.

by officially including related activities as main threats to national security. For the United States, certain competitors or opponents seek to improve both the methods for striking combat networks and the operational concepts while using other ways of openly conducting the war for the purpose of achieving objectives (for example through information warfare, subversion, development of proxy operations)[4]. The decrease in the costs of accessing the global Internet network, coupled with the unprecedented development of portals, has led to the exchange of information, in the form of messages or video content and images free of charge, leading inherently to the dissemination in the information environment of the actions carried out by state actors or organisations, terrorists, but not limited to them and which are not traditionally capable of carrying out conventional actions against the United States. One feature of information warfare considered by the provoking actors when carrying out actions is represented by the mode of operation. In this regard, we identified the following approaches:

- openly – a strategy chosen for the dissemination of messages and associated media products, through vectors assumed by the provoking actor, both from the point of view of its origin (the audience being aware of its nature) and the topics promoted (these are channelled in totality to the direction assigned). In this case, it may be the situation with a hub vector from which they will be subsequently taken over in order to amplify topics or ideas;
- by a controlled intermediary – it implies the use of an intermediary vector (or several), situation in which it presents itself to the audience as independent, in fact being controlled to a certain extent by the provoking actor, promoting the themes entrusted by it. In this category we can include vectors whose formal attitude is quasi-known to the audience, but which does not promote themes oriented entirely towards the assigned direction;
- by an independent intermediary – in this situation the vector is claimed as being independent in front of the audience being quasi-recognised as such, the themes mediated by the vector are generally other than those promoted by the actor. Two other distinct sub-directions of action can be identified in this case: the theme promoted by the actor is disseminated unconsciously in the information environment by an intermediary, similar to the Leninist idiom *useful idiot*, or the dissemination is carried out following other actor-intermediary arrangements and which they can wear different

4 ***, *Summary of the National Defense Strategy of the United States of America 2018*, p. 3, https://dod.defense.gov›Documents›pubs›2018, retrieved on 17.07.2019.

shapes. We believe that this method has a high degree of effectiveness, especially in the peace phase of the conflict, because such vectors have a high degree of credibility for large audiences;

- covertly – it involves the dissemination of media products related to the topics pursued by the provoking actor through vectors under his control, that operate in an unassuming manner, and the audience does not realise their orientation. The themes pursued by them are entrusted and controlled directly by the actor.

Regarding the Russian Federation, among the main threats to national security, there are mentioned the activities related to the use of information and communication technology in promoting fascist ideology, extremism, terrorism, separatism and endangering political and social stability in society[5]. Therefore, in this case, we can also observe the subject areas, formally specified, and which have a high degree of susceptibility to be used in information warfare against the Russian Federation. Moreover, it can be considered that the state has set itself a position of superiority in the field, considering that from the perspective of promoting the national interests of the Russian Federation and realising the national strategic priorities, the foreign policy will seek to strengthen the position of the Russian mass media and the communication instruments of the Russian media in global information environment and transmitting the Russian perspective on international issues to a broader international audience[6].

THE OBJECTIVES OF INFORMATION WARFARE

The actions of the provoking actor in the information environment benefit from a reduced sensitivity in being labelled by the targeted state as hostile intentions associated to a certain extent with the conventional war. No international approaches have been identified to regulate these aspects, which hardly take positions in the situation of cyber-attacks with great difficulty. Therefore, it can be observed that the information warfare takes place in all phases of the conflict, moreover, we daresay to advance the that the actions of the information warfare are adequate to the state of peace. In this phase, the actions in the information environment are carried out with high intensity, going until the objectives that cancel the transition to the next phases of the conflict are reached. In such a situation we can claim

[5] ***, *Russian National Security Strategy*, December 2015, p. 3, www.ieee.es›OtrasPublicaciones›Internacional›2016, retrieved on 11.07.2019.

[6] ***, *Foreign Policy Concept of the Russian Federation 2016*, https://www.rusemb.org.uk/rp_insight/, retrieved on 11.07.2019.

with certainty that the objectives of the information warfare will be situated at the strategic level of the national interests, and the attainment of such goals will be done by influencing large audiences. This aspect is highlighted in the national security strategy of the Russian Federation, where the intensification of confrontations in the information environment at global level, caused by the aspirations of some states to use information technology and its associated fields in order to achieve geopolitical objectives, including by manipulating public perception and falsification of historical aspects, exerts a growing influence on the international situation[7].

A special case (through the high level at which it seems that the objectives involving the strongest opponents at global level were set) that we can give as an example, in the context of analysing the strategic objectives of the information warfare, is provided by the possible interference of the Federation Russian in the 2016 US election process. Although an official investigation is being launched by various committees of the US legislative system in this case, many of media outlets indicate an attempt by the Russian authorities to influence US presidential elections to undermine the Democratic Party. This approach was implemented through a combination of computer attacks that sought to penetrate the Democratic Party's computer systems later using data obtained in a disclosure campaign through the WikiLeaks portal, supported by a virulent social media campaign. This example argues that the objectives pursued by the information warfare are much more complex, bolder and more dangerous than those pursued by conventional war, especially those executed at the strategic level.

For operational and tactical levels, objectives may be designated specifically for information warfare, but these coincide with those in the fields of psychological or information operations. In fact, we can understand this type of warfare as a prerogative of the information operations in the crisis and war phases of the conflict.

DEVELOPMENT OF METHODS OF ACTION

The problem of developing response solutions in information warfare is a matter of high complexity. It is difficult to evaluate the possible methods, since the effects of the adverse actions are obtained after long periods, and when the effects are obvious, these are difficult to address. Following the vote through the referendum on Brexit, several analyses were published that referred to actions carried out by an army of Russian trolls involved in sending hundreds of thousands

[7] ***, *Russian National Security Strategy*, December 2015, p. 5.

of messages through 3,800 accounts, in favour of Brexit[8], in order to influence the of voting process. If we consider these actions executed through the social media networks belonging to those specific to the information warfare and given that they have contributed to an extent difficult to evaluate accurately, it becomes obvious that the effect obtained can no longer be eliminated through actions in the information environment. Thus, the opportunity to launch the information warfare defensively can be questioned.

In some states, the actions of own institutions are aimed at reducing the effects produced by hostile actors in the information environment. Thus, in the Russian Federation, in order to maintain political and social stability, measures will be taken to increase the degree of protection of the population against the actions of influence by promoting harmful information from extremist and terrorist groups, special foreign services and propaganda structures[9]. This formal approach leads us to the development of a strategy for the concerted action of several state institutions or domain managers. Given that the information packaged in different forms is disseminated through specific platforms or portals on the Internet, several courses of action can be selected containing, for example, a combination of the following directions:

- actions based on continuous monitoring of the information environment for the early identification phase of the threat;
- conducting the analysis indicating data regarding the exposure of information to domestic audiences, probable effects, themes used, key communicators etc.;
- involvement of information operations structures in order to develop a response strategy;
- involvement of cyber structures for carrying out computer attacks on portals used by hostile actors in order to prohibit access to information;
- engaging structures for operations in the information environment with the purpose of drawing up messages, in the already mentioned forms, and operating the dissemination infrastructure to counteract or limit the effects of those transmitted by the provocative actor.

It is worth mentioning that part of the courses of action proposed above are executed by structures of the armed forces, and the fundamental problem that arises at this point is the legitimacy of employing such capabilities, especially in the peace phase of a potential conflict, considering that their involvement would take place at a later stage of the conflict.

[8] Matthew Field, Mike Wright, *Russian Trolls Sent Thousands of Pro-Leave Messages on Day of Brexit Referendum, Twitter Data Reveals,* https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/, retrieved on 02 August 2019.

[9] ***, *Russian National Security Strategy*, December 2015, p. 10.

CONCLUSIONS

The information warfare is a reality nowadays, it is in the unfolding phase, without making its presence felt by the civilian population, pursuing the achievement of strategic objectives. It exploits the innovations of the information society, which have become for many of us *modus vivendi*, and presents enormous accessibility to global audiences through the Internet.

It is necessary, considering also the examples offered, to draw up a national action strategy in an information warfare situation, which will allow the integration, training, intra and inter-institutional operation of those responsable of carrying out operations in the information environment. The difficulty in achieving this approach comes from the lack of concrete models implemented in other Alliance states and from the lack of understanding of how the armed forces can effectively contribute to actions in the information environment in peacetime.

We estimate that, in the information warfare, the field of information operations may have a leading role in its specific actions or may represent at least one contributing factor to the overall effort.

BIBLIOGRAPHY

1. ***, *Foreign Policy Concept of the Russian Federation 2016*, https://www.rusemb.org.uk/rp_insight/.
2. ***, *Joint Doctrine for Information Operations*, the USA, 1998, www.c4i.org.
3. ***, *Russian National Security Strategy*, December 2015, www.ieee.es›OtrasPublicaciones›Internacional›2016.
4. ***, *Summary of the National Defense Strategy of the United States of America 2018*, available at *https://dod.defense.gov›Documents›pubs›20*18.
5. Matthew Field, Mike Wright, *Russian Trolls Sent Thousands of Pro-Leave Messages on Day of Brexit Referendum, Twitter Data Reveals*, https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/
6. Vasile-Dumitru Ionițoiu, Mihai Videscu, *Contrainformații în epoca post-adevăr*, Revista *Infosfera* no. 1, București 2018, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/index.php.
7. John Naisbitt, *Megatendințe*, Editura Politică, București, 1989.

ANTI-AIRCRAFT DEFENCE AND HYBRID THREATS

Florin STAFI
PhD Candidate, "Carol I" National Defense University, Bucharest

The hybrid forms of manifestation of war characteristics are difficult to counteract, to analyse and almost impossible to anticipate. The interactions being macro-systemic, all the architectural components of a state's security must calibrate their resources to design adapted reactions. Therefore, each component is required to self-evaluate its critical functions, and at the same time, to determine its own vulnerabilities in front of a two-faced enemy.

The identification of threat levels in emerging of air technologies is also the attribute of the anti-aircraft fire system, due to an important functionality in the multi-dimensional battlefield. Therefore, in an extremely complex equation of a different type of war, the specialised components of the anti-aircraft response will vectorially redefine their force instruments, concentrating their effort to create synergy in effects. Accepting the hybridisation of war must transcend the Clausewitzian symmetrical classicism, especially since, in many ways, the forms and methods of manifestation are not new. It remains, however, to accept that the appropriate reaction to such a possible war can only be achieved through a complex understanding of the phenomenon, beyond the restrictive barriers of previous tactic or strategy.

Keywords: hybrid warfare, anti-aircraft, technology, armed conflict, proxy war.

INTRODUCTION

The confrontation, conflict or struggle between two organisations has existed throughout time everywhere. Whether we are talking about the economic, financial, military or diplomatic field, they have one purpose: to make a *"profit"*, by imposing the will of one of the parties. In a generalist approach, the existence of two forces, with antagonistic intentions, which channel their energies, visible or not, through their own strategy, vectorised by the available means, is admitted.

In extenso, we can talk about a war of interests, with previously established rules and statutes in a *Westphalian* manner. The laws are applied non-duplicitously, and the accepted principles are those that govern the further development of the actions. But what if one of the parties violates the good practices of the treaty of 1648, distorting that *code d'honneur* of the battlefield? The answer is apparently simple: adaptation!

It is often spoken, in the media of analysis of the phenomenon of war, that it has evolved at the same time with the society that generated it. From my point of view, I do not think that we can accept progress in itself, but only a circumstantial change, generated by many factors: convergent technology, geopolitical, geostrategic or economic interests, level of power achieved etc. Basically, the governance remained the same, only the methods and tools changed. This is why, in the conditions of a dissolution of the power centres of the last century (predominantly east-west), terms similar to this phenomenon have appeared: asymmetrical, proxy, irregular, guerrilla, informational or imagological. On the other hand, few wars have looked the same, and the differences are not few: in terms of objectives, protagonists (structural level), ways to fight, space of engagement or their combinations.

After all, none of the attributes has brought anything new. The war has always been asymmetrical; by its nature, as Clausewitz pointed out in the XIXth century, it is unpredictable, with a chameleonic aspect, and which, by reflecting the political characteristics that generate it, changes its appearance with each occurrence. Guerrilla tactics or even insurgency were not invented in the last century. General and strategist Sun Tzu, in *The Art of War* (6th century BC), was one of the first supporters of the use of guerrilla warfare. The earliest description of the guerrilla war is an alleged battle between Emperor Huang and the Myan (Miao) people of China[1].

[1] *"We might note that the first guerrilla war had been waged in 360 BC in China, when Emperor Huang was fighting the Miao race under Tsi Yao"*, Western Political Science Association, *The Western Political Quarterly: Volume 15*, 1962, p. 180.

The nomadic and migratory tribes, such as the Scythians, Goths, Vandals and Huns, used elements of guerrilla warfare to fight the Persian Empire, the Roman Empire and Alexander the Great. Quintus Fabius Maximus Verrucosus, widely regarded as the *"father of the guerrilla war"* of his time, designed the *Fabian* strategy that was used with great effect against Hannibal's army[2], war by interposition or proxy, as it is known now. In classical antiquity and in the Middle Ages, numerous armies, often irregular, were *external parties*, which were introduced into an internal conflict and aligned with a belligerent to gain influence and develop their own interests in the region. Some medieval states, such as the Byzantine Empire, have used the proxy warfare as a tool of foreign policy, deliberately cultivating the dispute between hostile rivals and then supporting them when they went to war with each other[3]. Other states considered proxy wars as a mere useful extension of a pre-existing conflict, such as France and England during the Hundred Years' War, both of which initiated a long-standing practice of supporting piracy, which targeted the commercial transportation of the other. Also, the Ottoman Empire used barbarian pirates as representatives to harass Western European powers in the Mediterranean[4].

Hybrid war is not a new concept either. Its echoes are found, among others, in the ancient writings of Sun Tzu, Kautilya or Thucydides. The combination of conventional and irregular methods has been used throughout history: the campaigns carried out in ancient Spain by the Lusitanian leader Viriathus or the renegade General Sertorius against the forces of the Roman Republic in the 2nd and 3rd centuries BC. Elements of hybrid warfare are also seen in the concept of *petite guerre*, a kind of recognition today practised by light troops in European armies in the seventeenth and eighteenth centuries.

The staging of the typology of the war is difficult to achieve. Analogies have been made between the industrial revolutions and the forms of manifestation of the armed conflict, insisting, *post factum,* on the patterns of the development of the war. There is nothing wrong, just that it is impossible to reproduce at scale the mechanistic representation of such a large phenomenon. The connection between these two resides implicitly in the *living* substance, the technology. Whether we are talking about longbows, gun powder, tank, submarine or UAV, these being just a few examples, we must accept that the changes in the form of manifestation of the strategy – the ideological support of the war – were a consequence

[2] Walter Laqueur, *Guerrilla Warfare: A Historical & Critical Study*, Transaction Publishers, 1976, p. 7.
[3] Geraint Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics,* Sussex Academic Press, Brighton, 2014, pp. 5, 12-13.
[4] William Watson, *Tricolor and Crescent: France and the Islamic World*, Praeger Books Westport, Connecticut, 2003. pp. 17-19.

of the access to the *new weapon*, to which the manoeuvre, number of combatants, tactics used etc. were adapted, without a doubt. And if today we are at the peak of technology, in full *revolution 4.0*, the implications on the typology of war can only be overwhelming. The numerous risks associated with technological evolution can affect the structural functioning of the states, generating a feeling of vulnerability through their destructive potential.

Taking into consideration the hybrid side of a war, we must admit that it has the potential to transform the strategic calculations of the potential belligerents, due to the increase of the number of non-state actors, the technology, the multi-dimensionality of the space of employment and the proliferation of advanced weapon systems. As a result, the air domain is increasingly being exploited to carry out terrorist attacks, the means used thus representing a significant threat to internal security and national defence. A wide range of airborne devices appear as potential threats, both for the safety of combatants and/or critical infrastructure or even to produce significant cognitive effects, and among the civilian population. Moreover, assimilated, easy to obtain, commercial technologies (drones, balloons, light gliders, etc.) have greatly improved the air capacities of state/non-state actors, thus broadening the range of air threats. As a result, the role of the anti-aircraft fire system becomes (again) much more emphasised/taken into account, both on the prevention side, but more especially on the combat one. *The expectation* of an air enemy will be more difficult to calculate, the attack procedures will no longer respect a pattern configured by the technical-tactical characteristics of the classical means, thus imposing a structural, doctrinal and actional retransformation of the component elements of the artillery and anti-aircraft missile structures.

HISTORICAL AND CONCEPTUAL LANDMARKS OF THE HYBRID COMPONENT OF THE WAR

The hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilise countries. Others use it to destabilise them.

Jens Stoltenberg, NATO Secretary General, 2015

In the specialised literature, the term hybrid warfare does not have an acknowledged definition, being used by many analysts of the phenomenon of warfare in the most different ways. Some refer only to irregular tactics, others describe it as a combination of conventional and unconventional actions in the same battlespace, some in order to redefine a new doctrine or even to justify the lack of reaction in the face of aggression of a *different* kind.

Calling for semantics, **the hybrid** is: **either** the result of a crossing between two genders, different varieties/races, having characteristics of both; **or** heterogeneous

elements, disparate/random (from two or more entities) and combined, apparently without any logic. Therefore, the hybrid is something different from the primary sources, having structural (genetic) changes, but, in essence, performs the same functions as the original.

Bringing together the terms hybrid, for example, and war, resulting in the expression *hybrid war*, may change the meaning of the base, assuming, *a priori*, that it is regulated by axiomatic characteristics, deeply demonstrated by science. But can we talk about a totally scientific war? Does it change its own behaviour, or there is only a difference in means and ways to go, the purpose remaining the same?

The paradigm of hybridising modern warfare reappeared with the Ukrainian-Russian conflict (2014), when, under the pretext of restoring constitutional order in Ukraine, soldiers without military insignia (green men), partisans of the Kremlin regime, carried out military actions in Crimea. The final result is known, the secession of the peninsula and its annexation to Russia. Subsequent escalation of the conflict determined Frank Hoffman to (re)define the concept of hybrid warfare as "*the simultaneous use by an adversary of conventional weapons, irregular tactics, terrorism and criminal behaviour, in the same battlespace, to achieve political goals*"[5]. Previously, the same author, in *Conflict in the 21st Century. The Emergence of Hybrid Wars*, underlined the impressive future adaptability of some state and/or non-state organisations to prepare and use, in a new conception, different capacities and asymmetric methods, simultaneously with the classic ones[6].

Focusing on gaining and maintaining long-term political victory, the manifestation of conflictuality within this type of war takes place not only in the military sphere. As a reference to Liddel Hart's great strategy, the basic characteristic acquires multi-modal features, with systemic interactions in all the means of manifesting political, diplomatic, economic, social, educational, health, and so on, interests. In other words, it is a conflict with several latent outbreaks, with difficult to anticipate evolutions, but also a harder to counter one. Therefore, hybrid conflicts have a broad range of manifestation, both with physical and conceptual dimensions: the first, a fight against an armed enemy, and the second, population control, by any means and ways.

[5] Andrew Radin, *Hybrid Warfare in the Baltics. Threats and Potential Responses,* RAND Corporation, Santa Monica, available at http://www.rand.org./content/dam/rand/pubs/research_report/RR1500?RR1577?RAND_RR1577.pdf, retrieved on 20 August 2019.

[6] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for policy Studies, Arlington – Virginia, December, 2007, p. 27 *apud* V. Cruceru, *About the Concept of Hybrid Warfare in American Military Thinking,* in Bulletin of the *"Carol I"* National Defense University, București, 2014, p. 30.

However, the hybridisation of war does not have its origins in this century. In their attempt to win a war, ancient Chinese rulers pursued a *four-methods* approach: using barbarians against barbarians, hiring mercenaries, building strategic alliances and dividing (imposing) areas of influence[7]. *Next best is to disrupt his alliances*, said Sun Tzu in the *Art of War*[8]. The strategic thinking of ancient China, focused on the above work, presents the fundamental principles of the hybrid concept: the use of deception and informants (spies), the mixed use of regular and irregular troops, and, last but not least, the focus on defeating the will of the enemy to fight.

In a similar way, Kautilya presents in *Artashastra* the characteristics of a hybrid war. *First, they will hit the allied armies on the forests, the cities and the enemy's ally. [...] the abundance of traitors is an additional reserve for the enemies. [...] I will force those armies who left the enemy to fight against cities or forests*[9].

A brief overview of some important battles in history supports the argument that a combination of conventional and unconventional in combat is not the exclusive feature of the 21st century. Here are some landmarks: the Peloponnesian Wars (431-405 BC), the Franco-Indian War (1755-1763), the US Independence War (1763-1791), the Spanish or Peninsular War (1807-1814), Garibaldi's campaign in southern Italy (1860-1861), the British campaign against the Ottoman Empire during the First World War, the Vietnam War (1955-1975) and others. All of these have in common: using unconventional weapons/tactics/rules in a conventional template of the time; surprising the opponent by knowingly violating some so-called rules of conduct on the battlefield; influencing, *ante factum*, the outcome of the war, by using any means available to it; exploiting the breaches of the security strategy of the enemy state. For example, King Brasidas has achieved, almost 2,500 years ago, a strategic advance of 400 km – unthinkable for that time – using, to a large extent, mercenaries. Also, through its strategic conception, he aimed, through military and diplomatic means, to break up allies in the northeast of Athens from the mother city. The Peloponnesian wars provided a shining example of how military goals and methods must be combined with political ones, being practically the temporal landmark of the emergence of a nuanced strategy, which did not always follow the immediate battle.

The hybrid characteristics of war were not only obvious in inter-state conflicts. Israel is permanently in a readjustment of strategy in front of the irregular actions,

[7] Benjamin David Baker, *Hybrid Warfare with Chinese Characteristics*, in *The Diplomat*, 23 September 2015, available at https://thediplomat.com/2015/09/hybrid-warfare-withchinese-characteristics/, retrieved on 20 August 2019.

[8] *** *Pages from Universal Military Thinking,* Editura Militară, București, 1984, p. 231.

[9] *Ibid*, pp. 252-253.

focused not only on military objectives, and carried out by Hezbollah, Fatah and Hamas, increasingly modernised and technologised terrorist groups. Often, the IDF has been unprepared for *hybrid* enemies by opposing only conventional means. In many situations, Hezbollah engaged Israeli forces in a seemingly symmetrical fight, but used irregular tactics at the same time, including positioning small units in overcrowded cities/centres, precisely to counter the enemy's firepower. In this way, a non-state actor traditionally classified as a terrorist organisation has demonstrated an incredible ability to mix classic military capacities with insurgency-specific ones.

Gerasimov's doctrine, on which the Kremlin's intervention in Ukraine was based, considered eminently hybrid, seems to have its origins, in fact, in an older conception, belonging to Russian military theorist Evgheni Messner (1891-1974), a Colonel in the General Staff of the Tsarist army. Author of *meatejevoina ("war of insurgency"),* Messner established that the main attributes of this type of conflict are: unconventional and unorthodox character, ambitious strategic design, planned and executed with professionalism, expanded and gradual, based on war doctrines, but also on nihilistic principles. The objective of the *"insurrectionary war"* is to induce panic in the mind of the enemy, distrust of the leaders, of their own forces, opinions, feelings and the demoralisation of troops and population[10]. At the beginning of 2014, one year after Colonel General Valery Gerasimov drew attention to *"changing the rules of the war"*, in the sense of increasing the role of non-military instruments in achieving political and strategic goals, the head of the General Operative Direction of the General Staff of the Russian Army, Colonel General Vladimir Zarudnitzki, captured the essence of hybrid war in a statement made at the Third Conference on International Security in Moscow: "*To divide a state from within is easier than to conquer it with weapons"*[11]. It sounds so much like Sun Tzu and Kautilya almost two millennia ago!

According to the current version of the Russian military doctrine (adopted in 2014), influencing the enemy *"throughout its all territory and, simultaneously, in the global informational space"* is one of the characteristics and particularities of the current armed conflicts. According to the doctrine of informational security (2016), among the methods of ensuring the information security in the field of defence, there is the neutralisation of the informational-psychological pressures, which includes *"undermining the historical bases and the patriotic traditions of defence"*[12].

[10] F.M. Nicolescu, *The Hybrid War. Russian Conceptual Perspective,* in *Intelligence Magazine*, 18 December 2017, in https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa/, retrieved on 21 August 2019.

[11] *Ibid.*

[12] *Doctrine of Information Security of the Russian Federation*, 5 December 2016, available at afyonluoglu.org/PublicWebFiles/strategies/Asia/Russia%202016%20Information%20%Security%20Doctrine.pdf, retrieved on 15 July 2019.

Dissertations on war hybridisation are broad and difficult to cover in one article. As in a mirror room, the perceived image can often be distorted, difficult to reproduce, difficult to understand and impossible to tell from the original. Many historical examples make us wonder if the exception was the classic, the duel with equal weapons, and the hybrid manifestations are the rule!

Perhaps the phrase *hybrid warfare*, in the current conflict situation, is too vague or too meaningless, leading us to think of something distorted, out of the classic patterns, without logic. In reality, the hybridisation of the war takes place on a *continuum* of competition between two or more actors, in the non-militarised phase, which must, however, create the premises for the success of the future conventional aggression.

Instead of concluding, I will present some of the essential characteristics of the hybrid warfare, which I think can later influence the way of action of the artillery and anti-aircraft missile structures in the Ground Forces. These include: the capacity of a party to employ a combined tactic; the simultaneous use of several types of units/insurgents (regular forces, special forces, partisans and mercenaries); the use of small structures, flexible, adaptable and with high reaction capacity; use of advanced technology, for purposes other than those for which they were built; terrorist attacks in all areas of action/propagation; conducting a misinformation, propaganda and media control campaign; supporting criminal groups; information control and superiority; creating diversions among the local population; duality of the final objectives: stabilisation vs. destabilisation, security vs. decentralisation, reconstruction vs. dismembering. As such, their study and analysis is extremely difficult to accomplish, especially on a classic operational framework. The centres of gravity must be permanently translated and analysed, being very volatile in instruments, and their protection and neutralisation, respectively, is a complex, flexible, adaptive and discouraging political-military strategy.

THE SYSTEMIC ROLE OF AIR DEFENSE IN HYBRID WARFARE

In the context of hybrid threats, the antiaircraft defence is mainly used to provide adequate support to manoeuvre forces in their actions on the ground. Practically, nothing changed from the tasks assimilated/deduced from the mission for which it was created. However, it seems increasingly necessary to reflect on this aspect in the conditions of the re-evaluation of the hybridization paradigm of current or future conflicts.

Starting from the necessity of limiting the effects of the hybrid character of the war and determining the systemic role of the reaction of the air defence, we must find and motivate the answers to the following questions: *What is the meaning*

of the hybrid action?; What are the threats, How can they evolve and how can I counter them? What is the maximum level of risk assumed? In what turning points does the centre of gravity need to be reassessed?

Considering the lessons of the past, I can say that the logic of waging a different kind of war exposes its reasons by: the tendency towards gaining/maintaining/imposing the zones of economic-military influence, the segregation of the poles of power and the passage towards multipolarity, the expansion of globalisation, the increasing state interdependence (by defining interests) and, last but not least, easy access to technology. All of these lead to: precarious balance of power, power diffusion, challenging national *status-quo*, increasing regional (even continental[13]) vulnerability, easy access to efficient technological means available to create diverse threats. Taken together, these tendencies converge towards providing opportunities for revisionist states, which can thus develop new hybrid warfare techniques by combining non-military and military means and involving diversified classes of non-state actors.

The traditional, Clausewitzian analysis of the threats of a hybrid war must be extended to all the PMESII-PT[14] component elements. In this regard, we must accept the following: the hybrid feature uses MPECI[15] tools and techniques much more diversified and more difficult to estimate; the vulnerabilities are systemically assessed and evaluated, looking for profound social effects; effects synchronization takes place in different ways than the classical ones; only the simple estimation of the instruments of power of a possible enemy does not reflect how they will be used; hybrid warfare intentionally exploits **ambiguity**, thus instilling **creativity** (as an intuitive antidote!) [16]; the technology is the multiplier factor of the created effects. On this model/analytical framework all the resources (attacker vs. defender), concentrated by the strategy to exploit the vulnerabilities, synchronise the effects by prior realising the congruence of the systemic actions.

Referring strictly to the threats corresponding to the actions of the air defence, I can say that they have become increasingly diversified, both as products themselves and as a domain of action. Thus, a large number of aerial devices exceeded the commercial threshold and entered the combat arsenal of some states/organisations. The so-called LSS (Low Slow Small), these unmanned aerial vehicles (drones, RPVs,

[13] See the impact of the flow of migrants on the states of Europe, the economic and financial point of view, in http://publications.europa.eu/webpub/com/factsheets/migration-crisis/ro/

[14] **PMESII-PT** is an acronym developed by US military doctrine and refers to political, military, economic, social, informational, infrastructure and time factors.

[15] **MPECI** – Military, Political, Economic, Civil, Informational, in *MCDC Countering Hybrid Warfare Project: MCDC February 2019 Countering Hybrid Warfare* available at https://www.ugr.es/~jjordan/MCDC-Countering-%20Hybrid-Warfare.pdf, retrieved on 22 August 2019.

[16] See the deployment of the Lebanon's military campaigns listed above.

hot air balloons, gliders, etc.) have greatly improved the warfare capacity (by airpower) of some actors and which, coupled with the possession of classic aircraft, extend the definition and methods of employing what we know as "*Renegade*". For example, in August 2019, Israel used two armed drones (possibly a mini-UCAV) to destroy a Lebanese rocket factory controlled by Hezbollah[17] supporters.

Another example, in which Tel Aviv was not involved, took place in December 2017. Fifteen drones attacked the Khmeimim Russian airbase in Syria, apparently destroying a number of aircraft and destroying other military equipment[18]. Russia claimed that a state actor was behind the attack, but many intelligence agencies have held a non-state actor responsible (probably Hezbollah, in response to backing the Damascus regime supporters).

At the same time, emerging technologies, with rapid development, have given birth to new fields such as cyberspace, where military, national or international rules have not yet been created. Space (as a dimension) is no longer a frontier, but an operating environment, with increasingly diverse features and interactions (cultural, technical, informational), which, *in fact*, provide new tools for influencing traditional security thinking. Notable, cyberspace is a dimension that could be used to allow the evolution of hybrid threat, especially due to the need for network working. A particular aspect is the invasive feature in existing networks, even in peacetime. In this regard, both the use of cyber capacities and LSS can affect an anti-aircraft fire system, without prior notification and under complete anonymity.

Of course, there are other (generic) threats assimilated to the hybridisation of war and that can also trigger reactions from the component systems of the air defence: so-called *fake news* – influencing not only the morale of the troops but also the decision-making capacity of the commanders –, the existence of terrorist organisations masked in other forms of activity, lack of ROE, the artificial intelligence or even proliferation of weapons of mass destruction (and especially easy access to them). Last but not least, the classic air platforms (aircraft, helicopters, ballistic missiles) close a complete circle of possible force instruments, able to contribute decisively, in all the stages of a war, to the achievement of the desired final state.

It is well-known that the only certainty in war is the presence of incertitude. The hybrid feature of a conflict emphasises this assertion, which is why I think it is necessary to create/assume a simple model of its absorption, including at the level of the systems that make up the air defence. Integrated in all phases of the conflict,

[17] Robert Fisk, *Lebanon's Crisis Is almost Unstoppable. Drone Warfare Is on the Horizon,* in *Independent*, 05 September 2019, available at https://www.independent.co.uk/voices/lebanon-israel-hezbollah-drones-syria-idlib-saad-hariri-hassan-nasrallah-a9093301.html, retrieved on 06 September 2019.

[18] *Haaretz*, 08 September 2019, available at https://www.haaretz.com/israel-news/.premium-armies-of-drones-are-being-set-up-all-over-the-world-and-israel-isn-t-prepared-1.7758575, retrieved on 08 September 2019.

it must redefine a systemic behaviour, through *the simple strategy of the five steps*, as follows: assessing emerging threats; identifying national critical vulnerabilities; issuing hypotheses regarding the capabilities and objectives of the hypothetical enemy; developing new warning indicators (to logically link the first three steps)[19]; finally, the derivation of the actions, effects and conditions necessary to combat the threats, in a comprehensive approach.

Apparently, the role of anti-aircraft defence component systems cannot differ much in a war with hybrid features. But, given both the potential threats and their own vulnerabilities, all within an actional logic of the hypothetical enemy, it may be necessary to address the role of ADA in a multi-systemic context, with an integrated national (or alliance) perspective, focused on the main phases: detection, evaluation, execution, transition. A number of technical measures could be possible, as follows: multilayer ISR, integrated in a common C2 operational architecture, especially for LSS; merging and managing a large amount of data; involvement of non-traditional (civil) ISR instruments; creating models for predicting air threats; approaching the decision cycle on a heuristic model (represented); creation of direct warning links between specialised information agencies (even civilians, according to the American model) and AD component systems; harmonising procedures and developing a common, integrated vision; integrating all the key capabilities for effective defence of the national territory, population and critical infrastructure (Home Air Defense).

CONCLUSIONS

No doubt, in the future, hybrid opponents will be a challenge not only quantitatively but also qualitatively. Even if, organisationally, they will be bigger or smaller (such as Hezbollah today), they will certainly be more disciplined, organised and with a higher command-control capacity than today. They will make up for the lack of quantity with the firepower generated by increasingly sophisticated military equipment, which can act in all battlefields. In response, counteracting their actions will require competences quite different from those needed, for example, for counterinsurgency.

No one can know if the future conflicts will be, *quasi generalis regula*, conventional or hybrid. Certainly, these will have strong nonlinear characteristics, difficult to predict, which will take different forms of strategy and tactics, with simultaneous attacks in different environments. This certitude derives precisely from the expansion of society (through globalisation and multi-culturalisation), the easy unconditional access to the virtual and cognitive dimensions of the war and the expansion, through the potentially destructive emerging technology, of the so-called *grey areas*.

[19] For example, the excessive use of drones by the Russian Federation in the Donbas campaign may be such an indication (n.a.).

Therefore, the present evolutions require a rapid adaptation of the military dimension of a democratic state, in order to be able to deal with any strategic surprise. There are several aspects that must be considered. First, access to information superiority, viewed not in the sense of quantity, but especially in the possibility of analysing a large volume of data in a very short time. Secondly, understanding the need to create systemic hyper-connectivity, in order to eliminate the decision overlaps, increase the flexibility, the ability to surprise the opponent, the availability and the optimisation of resources. Third, the rapid adaptation of users to new technologies, through the implementation of adapted educational programs. Last but not least, keeping a section dedicated to the human decision-making process, especially on crucial and determining topics. And finally, the acceptance that, in a future armed conflict, the degree of involvement of civil actors, difficult to track or control, is increasing.

The character of war in the future will change as frequently as it has in the past, but there will be many striking continuities, including terrorism and violent mass protest movements. There will almost certainly be a significant increase in irregular warfare, regular warfare and systemic warfare. I consider will be the following trends of future war: irregular warfare, especially in urban area exploiting the infrastructural vulnerability; porosity; dispersal; depth; stealth; miniaturisation of combat power; precision and privatization of violence[20].

The anti-aircraft defence, as a combat function, must **adapt** *to future threats, not only under the pressure of escalating of latent conflict outbreaks in NATO's border proximity but especially of the tendencies of technological development and use of new air devices. Trying to find new ways of influencing a way of thinking is extremely difficult, sometimes even impossible. However, what is possible is the limitation of its effects, through a correct prognosis, systemic reconfiguration and technological counterbalance. The anti-aircraft defence systems components must have their current tactical role recalibrated, understanding that maximum space control can become more important than ever, regardless of the nature of a future war.*

BIBLIOGRAPHY

Books

1. ***, *Dicționarul explicativ al limbii române*, Editura Academiei, București, 2012.
2. ***, *Pagini din gândirea militară universală*, Editura Militară, București, 1984
3. Ion Bălăceanu, *Revoluţia tehnologică contemporană şi impactul ei asupra potenţialului military*, Editura AÎSM, Bucureşti, 2001.

[20] Robert A. Johnson, *Predicting Future War* available at ssi.armywarcollege.edu/pubs/Parameters/issue/Spring_2014/6_Johnson.pdf retrieved on 23 August 2019.

4. Ion Bălăceanu, Daniel Dumitru, Ion Ioana, *Potențialul de luptă al Forțelor Terestre în context NATO,* Editura TOP FORM, Bucureşti, 2006.
5. V. Cruceru, *Despre conceptul de război hibrid în gândirea militară americană*, Buletinul Universității Naționale de Apărare *"Carol I"*, București, 2014.
6. Ferdinand Foch, *Principiile războiului. Conducerea războiului,* Editura Militară, București, 1975.
7. J.F.C. Fuller, *The Foundation of the Science of War,* The Camelot Press Limited Southampton, 1993.
8. B.H. Liddell Hart, *Strategia acţiunii indirecte,* Editura Militară, București, 1973.
9. Geraint Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics, Sussex Academic Press, Brighton, 2014.*
10. Walter Laqueur, *Guerrilla Warfare: A Historical & Critical Study,* Transaction Publishers, 1976.
11. Iulian Martin, *Interacţiunea strategiilor în conflictele armate modern,* Editura Universităţii Naţionale de Apărare *"Carol I"*, București, 2012.
12. Andrew Radin, *Hybrid Warfare in the Baltics. Threats and Potential Responses,* RAND Corporation, Santa Monica.
13. L.N. Rangarajan, *The Arthashastra*, Penguin Books, New Delhi, 1992.
14. Cristian Stanciu, *Viitorul conflictualității – operații asimetrice și hibride*, Universității Naționale de Apărare *"Carol I"*, București, 2016.
15. Sun Tzu, *Arta războiului*, Editura Militară, București, 1976.
16. William Watson, *Tricolor and Crescent: France and the Islamic World,* Praeger Books, Westport, Connecticut, 2003.

Publications

1. *Allied Joint Doctrine for Air and Space Operations*, Edition B, Version 1, 2016.
2. *Doctrine of Information Security of the Russian Federation*, 5 December 2016.
3. *HAARETZ*, 08 September 2019.
4. *NATO Glossary of terms and definitions*, 2015.
5. *NATO Glossary of abbreviations used in NATO documents and publications*, 2016.
6. *Intelligence* Review, 18 December 2017.
7. *The Diplomat*, 23 September 2015.
8. Western Political Science Association, *The Western Political Quarterly: Volume 15*, 1962.

Webography

1. http://www.nato.int, retrieved on 02 August 2019.
2. http://www.globalsecurity.org, retrieved on 15 August 2019.
3. http://www.nato.int/docu/review/index_fr.htm, retrieved on 15 August 2019.
4. http://www.rand.org./content/dam/rand/pubs/research_report/RR1500?RR1577?RAND_RR1577.pdf, retrieved on 20 August 2019.
5. https://thediplomat.com/2015/09/hybrid-warfare-withchinese-characteristics/, retrieved on 20 August 2019.
6. https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa/, retrieved on 21 August 2019.

7. http://publications.europa.eu/webpub/com/factsheets/migration-crisis/ro/, retrieved on 22 August 2019.
8. https://www.ugr.es/~jjordan/MCDC-Countering-%20Hybrid-Warfare.pdf, retrieved on 22 August 2019.
9. https://www.independent.co.uk/voices/lebanon-israel-hezbollah-drones-syria-idlib-saad-hariri-hassan-nasrallah-a9093301.html, retrieved on 06 September 2019.
10. https://www.haaretz.com/israel-news/.premium-armies-of-drones-are-being-set-up-all-over-the-world-and-israel-isn-t-prepared-1.7758575, retrieved on 08 September 2019.
11. ssi.armywarcollege.edu/pubs/Parameters/issue/Spring_2014/6_Johnson.pdf retrieved on 23 August 2019.
12. http://warfare.ru/catalog=true, retrieved on 12 September 2019.
13. http://www.nato.int/docu/basictxt/treatry.htm, retrieved on 12 September 2019.

STRATEGIC INTEREST OF THE RUSSIAN FEDERATION IN THE MIDDLE EAST – PART OF A "MASKIROVKA" TYPE STRATEGY –

Alexandru PINTILI
Instructor, Intelligence Defence Training Centre, Bucharesti

Marian ȘTEFAN
Instructor, Intelligence Defence Training Centre, Bucharest

To show interest in an area that appears to be under the influence and interests of others, the Russian Federation had to move away from the old paradigms and build viable strategies, not necessarily new ones, in order to achieve the surprise.

At first glance, the plan implemented by the Russian Federation seems to be something new, elaborate, innovative and carefully crafted. Partly this is true, we can talk about a rebranding strategy, but if we look closely at the strategies that are being addressed, we see the same attempts validated by the past experiences. We notice the same way of active involvement in others' problems, without being in contradiction with historical actions, now fighting on the same front with the old enemy of the frozen period, melted not so long ago and having, which is surprising for all analysts, the same invoked enemy: terrorism. It is a new type of fanatical terrorism, unwarrantable from the point of view of doctrine, but with territorial claims that give cold shots to the whole of Europe. Something similar for the common enemy for which the world, more or less civilised, more or less prepared, more or less involved, accepted to fight together, divided in two power and interest alliances, three quarters of a century ago.

Highlighting the intentions to support the common world effort to eliminate the terrorist threat and multiple forms of manifestation is part of the Russian Federation new strategic doctrine of misinformation, designed to gain strategic benefits. Until now, USA talks about "Maskirovka" like being part of "deception and denial" disinformation military plan used by the Russian Federation in order to mislead the opponent about the real intentions of using military actions. Now we have an appreciated form of this elaborate plan not to hide but to show real intentions and actions that hide real strategic interests.

What is the stake? We will see that the Russian Federation strategic interest stake is neither economic nor military, but simply the desire to be an active part of the strategic game.

Keywords: Maskirovka, strategic interest, disinformation, rebranding strategy, terrorism.

In recent years, Russia has been conducting a highly sophisticated, well-funded and successful campaign to expand its global influence to the detriment of the United States. The leaders in Moscow have pursued a series of strategic objectives to undermine the liberal international order, especially in the areas of influence of the United States. Russia has demonstrated its return as a global superpower promoting its commercial, energy and military interests.

It can be noticed that Russia is trying to create a multipolar world, in which it plays a prominent role. Washington and its allies are forced to anticipate and analyse Russia's future courses carefully and in a concentrated manner. In order to expand its global footprint and to exert its influence, Russia relied on various diplomatic, cyber, military, energy, commercial and financial instruments.

For many years after the Cold War, Europe and the US have not paid much attention to Russia's efforts to expand its economic, military and political influence beyond its borders. Following Vladimir Putin's return to the Russian presidency in 2012, Russia has launched a sophisticated and well-prepared global outreach campaign. All this has led to Vladimir Putin's increasing internal legitimacy by demonstrating Russia's status as a global superpower.

In 2014, the undeclared war in the Crimea area and Russia's annexation of the peninsula led to tarnishing the international image of Western democracy. It is for the first time, after the breakup of the Soviet Union, when the US faces a Russia that tries to project its influence and to overcome its periphery through its presence in other areas of the world.

The regional crises in Asia and the Middle East have prompted the US and its allies to focus their attention on the area, but at the same time they have awakened Russia's interest, the latter taking advantage of and extending its influence and presence, using the Trump presidency' *"America First"* policy.

We can divide Russia's global activism into 4 geographical regions. Although there is some uncertainty about the motivation behind these efforts, in general, the ordering of Moscow's priorities closely aligns with the perception of Russian threats.

First of all, it emphasises the countering of Western influence in the former states of the Soviet Union. Moscow wants to control its neighbours to prevent them from approaching the West. At the same time, Moscow wants influence coverage in Central Asia, an area where China dominates economically.

Secondly, undermining the main adversaries: the US, the EU, NATO. The motivation behind the anti-Western actions is also fueled by the widespread view of Russia's security institution that the administrations of former presidents, George W. Bush and Barack Obama, have sought ways to weaken Russia internally and undermine its influence internationally.

Third, Russia's commitment to gain or regain influence in areas of the Balkans and the Middle East becomes obvious. Russia makes known its high-power status and its ability to act beyond its immediate vicinity through its intervention in Syria.

Russia is not seeking to become a major leader in the Middle East, but to accumulate as much influence in the area as possible. This may facilitate collaboration with the US in the Middle East in exchange for concessions in other areas. And if the US does not accept it, Russia will at least create a much more difficult situation through the influence gained in the region.

And last but not least, the attempt of the Moscow leadership to gain influence in different areas of Africa, Asia and Latin America by cultivating authoritarian leaders and forming growing coalitions of powers that challenge the international system influenced by the West.

The exercise of Russia's influence in Eurasia determined the connection to Moscow from the political, economic and security point of view of the neighbouring states and ensured the regional domination by Russia. The overall reach of Russian foreign policy is broader than expected. An illustration of this is how Moscow aspires to exert influence through various multi-lateral organizations with member states and affiliated partners both in the post-Soviet neighbourhood of Russia and in Asia, Europe and the Middle East (see *table 1*)[1].

Table 1: Members and partners of Russia-friendly multilateral organisations

Collective Security Treaty Organization (CSTO)	**Commonwealth of Independent States (CIS)**	**Eurasian Economic Union (EAEU)**	**Shanghai Cooperation Organization (SCO)**	
Member States	Member States	Member States	Member States	Dialogue Partners
Armenia	Armenia	Armenia	China	Armenia
Belarus	Azerbaijan	Belarus	India	Azerbaijan
Kazakhstan	Belarus	Kazakhstan	Kazakhstan	Cambodia
Kyrgyzstan	Kazakhstan	Kyrgyzstan	Kyrgyzstan	Nepal
Russia	Kyrgyzstan	Russia	Pakistan	Sri Lanka

[1] P. Stronski, R. Sokolsky, *The Return of Global Russia: An Analytical Framework*, in Carnegie Endowment for International Peace, 14.12.2017, <https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003>, retrieved on 05.08.2019.

Collective Security Treaty Organization (CSTO)	**Commonwealth of Independent States (CIS)**	**Eurasian Economic Union (EAEU)**	**Shanghai Cooperation Organization (SCO)**	
Member States	Member States	Member States	Member States	Dialogue Partners
Tajikistan	Moldova		Russia	Turkey
	Russia	Select to negotiate free trade	Tajikistan	
Observers	Tajikistan	Vietnam (FTA concluded 2015)		Aspiring observers and dialogue partners Bangladesh
Afghanistan		Egypt (in progress)		Bangladesh
Serbia		India (in progress)	Observers	Egypt
		Iran (in progress)	Afghanistan	Iraq
		Israel (in progress)	Belarus	Israel
		Mongolia (in progress)	Iran	Maldives
		Serbia (in progress)	Mongolia	Syria
		Singapore (in progress)		Ukraine

Source: The official sites of these multilateral organisations[2]

At the same time, Moscow's leaders continue to cultivate relations with Turkey. Russian-Turkish relations have improved quite rapidly after the drastic decline of 2015-2016, when Turkish aviation shot down a Russian fighter jet. All restrictions resulting from the incident were eliminated by early summer 2017.

Over time, there have been noticed a series of Russia's attempts to take advantage of the separatist tendencies in Eurasia. Moscow has also tried to re-establish and expand its presence in regions where it enjoyed great influence during the Cold War, the Middle East and South-West Asia.

[2] Alison Smale, *"Latvia's Tension with Russians at Home Persist in Shadow of Ukraine Conflict"*, in *New York Times*, 23 August 2014, https://www.nytimes.com/2014/08/24/world/europe/latvias-tensions-with-russians-at-home-persist-in-shadow-of-ukraine.html?_r=0.

The involvement of the Russian armed forces in Syria, starting from October 2015, has been a major escalation of the Russian support offered to the Syrian government and the first large-scale military operation, outside its borders, in the history of post-Soviet Russia. Prior to this, Russia's support for Assad was largely limited to diplomacy, financial aid, information exchange and delivery of weapons and equipment. Also, Russia has long kept military facilities in Syria, which would have been in danger if the Assad regime collapsed[3].

Although the intervention in Syria could have caused substantial losses to Russia, it can be seen that it was a real success. In this way, Russia has ensured its political and military presence in the Middle East and in the Mediterranean area in a manner that has not been seen for almost a generation.

Moreover, the Kremlin helped the Assad regime by preventing its collapse and stopping what was alleged to be an illegal US operation. Russia intervened in Syria for two reasons: to gain influence in the region in the event that the US would make concessions in other areas for cooperation in Syria and to prove to the world that Russia is still a great power.

With the operation in Syria, the Kremlin did not wait and took advantage of an opportunity to show its influence in Libya. The civil war generated by the NATO intervention in 2011 and the overthrow of the regime of former leader Muammar Qaddafi offered Russia a new opportunity to expand its influence. The Kremlin has long been critical of NATO's intervention in Libya, accusing the alliance of changing the regime under the guise of humanitarian intervention. Amidst the chaos of the Libyan civil war, Russia has partnered with a powerful local leader, Khalifa Haftar, whom France and the United States have also tried to cultivate as a local partner[4].

Moreover, the leaders in Moscow also noticed another opportunity to expand their influence, thus launching a partnership offer to the government of Egypt. This partnership led to a series of visits by Putin to Cairo and Abdel Fattah el-Sisi to Moscow and to joint military exercises. At the same time, an agreement on the purchase of Russian armament by the Egyptian army was also discussed, the latter being engaged in the fight with ISIS supporters from the north of the Sinai Peninsula. While the US Congress often opposes arms supplies due to human rights concerns, Moscow's leaders do not have this problem. Also, in 2017, Moscow sent some

[3] Inna Lazareva, *"Russia Spybase Used to Monitor Rebels and Israel Seized"*, in *Telegraph*, 8 October 2014, http://www.telegraph.co.uk/news/worldnews/europe/russia/11148857/Russian-spy-base-in-Syria-used-to-monitor-rebels-and-Israel-seized.html.

[4] Guma el-Gamaty, *"Is France Paving the Way to Haftar's Return in Libya"*, al-Araby al-Jadeed, 3 August 2017, <https://www.alaraby.co.uk/english/comment/2017/8/3/libya-is-france-paving-the-way-to-haftars-return>, retrieved on 06.08.2019.

of its special forces to support Egypt on the border with Libya. For this reason, Egypt's acceptance of Russia's position in Syria should not surprise anyone.

At the end of 2017, Putin and Sisi reached an agreement whereby Russia committed itself to building a nuclear power plant for Egypt, with total costs of about $ 30 billion.

In Syria, Libya and Egypt, Russia has shown its ingenuity, diplomatic agility and complete lack of scrupulousness in achieving its goals. In other areas, such as Iraq, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates, Moscow has launched diplomatic offensives[5]. The Kremlin has used a variety of means, including visits by senior officials, energy diplomacy, trade and economic ties, arms sales and civilian nuclear power projects to expand its influence and presence, signalling that Russia is returning to the Middle East as a major power and intends to remain in the long run. (The figure below gives a picture of Russia's expansion into the Middle East, the Black Sea and the former nearby Soviet states)[6].

For the Kremlin leadership, the concept of Maskirovka, traditionally, represents the use of military deception. The annexation of the Crimean Peninsula and the incursions by the Russian army in eastern Ukraine, as well as the intervention

[5] Sam Ramani, *"How Russia is Courting the Gulf"*, in *National Interest*, 1 August 2016.

[6] Paul Stronski, Richard Sokolsky, *op. cit.*

in Syria, is the beginning of Russian multidimensional challenges to NATO and its allies[7]. In Moscow, a new level of strategic ambition has been established, Maskirovka being redefined, applying misinformation at all levels of NATO command and by all possible means, all in order to keep the West unbalanced both politically and militarily.

Russia's goal is to block the distinction between influence, cooperation and competition by exploiting *"strategic ambiguity"* that is, the refusal of many European leaders to face the reality of the Kremlin's strategy and actions. The deception act is an eloquent statement of influence meant to force leaders who want to look west, to look further east. This objective is observed punctually in the recent military exercises of Russia, which involve the political circumstances of the states of Western Europe and the nuclear intimidation of the allies[8].

Although Russia's involvement is seen in areas of the Middle East, North Africa, South-West Asia, probably the main priority of the Kremlin leader is still Ukraine, perceiving US involvement in Ukraine's domestic policy in recent years as a threat. Russia hopes that, as the US will focus more and more in the Middle East, they will not be as attentive to Ukraine.

Following these actions, it can be concluded that President Putin is looking at a positive future for Russia. At the same time, from the point of view of the Kremlin leadership, the West is in decline, and the use of Maskirovka-type strategic actions can lead to an imbalance of the west and the goal of Russia, to create a new sphere of influence around its borders and in the ex-Soviet states and to end the "*frozen conflicts*" in the Middle East, Central Asia, North Africa and Eastern Europe in Russia's favour.

Analysing all these actions and intentions of the leaders of Moscow we can see that at present, Lenin's belief still works: if Russia cannot control a country, then at least it must be destabilised.

BIBLIOGRAPHY

1. M. Caliskan, *"Hybrid Warfare through the Lens of Strategic Theory"*, in *Defense & Security Analysis*, vol. 35, 2019.
2. Guma el-Gamaty, *"Is France Paving the Way to Haftar's Return in Libya*," al-Araby al-Jadeed, 3 August 2017, https://www.alaraby.co.uk/english/comment/2017/8/3/libya-is-france-paving-the-way-to-haftars-return.

[7] Julian Lindley-French, "*NATO: Countering Strategic Maskirovka*", Canadian Defence & Foreign Affairs Institute, May 2015.

[8] *Idem*, *"Countering Russia's Strategic Maskirovka"*, 24.09.2015**, <**http://lindleyfrench.blogspot.com/2015/09/countering-russias-strategic-maskirovka.html>, retrieved on 06.08.2019.

3. M. Jaitner, P.A. Mattsson, "*Russian Information Warfare of 2014",* the 7th International Conference of Cyber Conflicts, 2015.
4. I. Lazareva, "*Russia Spybase Used to Monitor Rebels and Israel Seized*", in *Telegraph*, 8 October 2014, http://www.telegraph.co.uk/news/worldnews/europe/russia/11148857/Russian-spy-base-in-Syria-used-to-monitor-rebels-and-Israel-seized.html.
5. Julian Lindley-French, *"Countering Russia's Strategic Maskirovka"*, 24.09.2015, http://lindleyfrench.blogspot.com/2015/09/countering-russias-strategic-maskirovka.html.
6. Julian Lindley-French, "*NATO: Countering Strategic Maskirovka*", Canadian Defence & Foreign Affairs Institute, May 2015.
7. A. Matveeva, "*Through Times of Trouble – Conflict in Southeastern Ukraine Explained from Within"*, Editura Lexington, London, 2018.
8. Sam Ramani, "*How Russia is Courting the Gulf*", in *National Interest*, 1 August 2016.
9. Alison Smale, *"Latvia's Tension with Russians at Home Persist in Shadow of Ukraine Conflict",* in *New York Times*, 23 August 2014, https://www.nytimes.com/2014/08/24/world/europe/latvias-tensions-with-russians-at-home-persist-in-shadow-of-ukraine.html?_r=0.
10. P. Stronski, R. Sokolsky, "*The Return of Global Russia: An Analytical Framework"*, 14.12.2017, available at https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003.

VULNERABILITIES AND THREATS FROM THE VIRTUAL SPACE VS. SECURITY ARCHITECTURES AT DIFFERENT LEVELS

Vasile Florin POPESCU, PhD

"Samoilă Mârza" Psychological Operations Centre, Bucharest

Different perceptions about the role and strength of the Internet are an important factor behind the lack of an international early warning mechanism in the field of cybersecurity. An opportunity to establish a framework for understanding the concept of cybersecurity would be to analyse cyberspace at different levels, each level indicating the consequences for different cyber-infrastructure disruptions. However, the consequences of cyber incidents and corresponding response mechanisms are quite different at global, regional and national level, and the cyber security issue has to be removed from the corner of the IT department, brought to the centre of the scene, and carefully supported by political attention and extra investments in order to modernise protection mechanisms.

Keywords: cyberspace, cyber threats, vulnerabilities, security architectures, early warning mechanism.

INTRODUCTION

Virtual or cybernetic space is a set of means and procedures based on information and communication technology (ICT) and consists of hardware, software, internet, information services and control systems becoming critical infrastructure for the socio-economic activity of any nation, a transnational organisation or project. Different dictionaries and encyclopaedias define cyber space as follows:

- cyberspace: a computer network made up of a global network of computer networks that use TCP/IP network protocols to facilitate data sharing (source: *Online Romanian Dictionary*);
- cyberspace is the electronic computer network environment where online communication takes place[1];
- a metaphor to describe the non-physical terrain created by computer systems: online systems create a cyber space where people can communicate with each other, research, or simply buy[2];
- Cyberspace is a field characterised by the use of electronic devices and electromagnetic spectrum to store, modify and exchange data through network systems and associated physical infrastructures. In fact, cyberspace can be considered as the interconnection of human beings through computers and telecommunication, regardless of geographic position[3].

The US Government defines the slightly wider cyberspace: Presidential National Security Directives no. 23 and 54 define cyberspace as the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, users, and those who control critical industries. The common use of the term also refers to the virtual information environment and interactions between people.

The definitions offered by Webster, Wikipedia, or the Oxford Dictionary are not absolute and comprehensive enough. The concept of virtual space has expanded in the meantime, including trade, finance, energy, stock exchanges and so on. The objectives of the attacks in the virtual environment can be classified into three major groups:

- the public sector, government agencies;

[1] *Wikipedia*, http://en.wikipedia.org/wiki/Cyberspace.
[2] http://www.webopedia.com/TERM/C/cyberspace.html
[3] http://searchsoa.techtarget.com/definition/cyberspace

- the private sector, mainly critical infrastructure operators;
- citizens.

The main threats associated with cyberspace can be classified into two main groups:

- threats to information and communications;
- threats to Information and Communication Technology Infrastructures -TIC.

Threats to information and communications are those that cause the loss, disclosure or misuse of information. The following threats can be listed among there:

- espionage – Within this category are included all types of espionage, from state espionage to industrial espionage;
- theft and publication of classified or sensitive information;
- theft and publication of personal data;
- theft of digital identity;
- fraud;
- Persistent advanced threats (AAP).

Threats to the ICT infrastructure are those that cause the temporary, partial or total disruption of some services or systems. Among these threats we can identify:

- attacks against critical infrastructure;
- attacks against networks and systems;
- attacks against internet services;
- attacks against industrial networks and control systems;
- virus infections;
- attacks against networks, systems or services through third parties.

Classification

Cyberattacks can be classified, depending on their source and impact, as follows:

❖ *Attacks sponsored by states*

The real world and physical conflicts have expanded into the virtual world of cyberspace. In recent years, cyberattacks have been detected against critical country infrastructures and specific targets. Some examples that are widely known by the public are: Estonia's cyberattack in 2007, which led to the temporary deactivation of a large part of the critical infrastructure of the Baltic countries, the cyberattack launched by Russia against Georgia in 2008 as a prelude to earthquake invasion, the Stuxnet case with cyberattacks against SCADA systems, the Duqu's case of cyberattacks against industrial organisations, the cyberattacks suffered by the US Government's classified networks by hackers in Chinese territory, and so on In recent years, some states have invested considerable economic, technical

and human resources in developing persistent advanced threats (AAP), aggressively attacking and choosing very specific goals, in order to maintain a steady presence within networks of possible victims. AAP attacks are very difficult to detect because they use techniques and components that are specifically designed to infiltrate remain in the network without being detected;

❖ *Attacks sponsored by private organisations*

The objective of many private organisations is to obtain industrial and economic secrets from other competing organisations, and this type of attack is often executed with government support;

❖ *Attacks of organised crime groups*

Organised crime gangs, also known as computer gangs, began to work in cyberspace, exploiting the possibility of anonymity that this domain offers. The objective of these types of gangs is to obtain sensitive information for their subsequent use of fraud and for significant economic gains.

❖ *Hackers*

With the advent of the Internet, but especially in recent years, hacker activities have become one of the greatest threats to governments and organisations of all kinds. The principles of this aggression are the anonymity and the free distribution of information through cyberspace, essentially via the Internet. Their mission is to "attack" the cyberspace of people, companies, projects, or other organisations that violate any of their principles or interests. This implies that the cyberspace of governments in most countries around the world, banks, telecommunications companies, critical infrastructure providers, Internet service providers, and ultimately all cyberspace are likely to be hacked with the goal to steal sensitive information;

❖ *Attacks of privileged (in-house)*

These groups are one of the greatest threats to the cyberspace security of nations, companies/projects because they are often an integral part of all the attacks outlined above from a spy infiltrated by a state or an employee who work for gangs of terrorists or cyber criminals, dissatisfied employees etc.

Levels and components

Virtual space or cybernetics is structured over three layers: a physical layer, a logical layer and a social layer, which are in turn composed of five components: the geographic component, the physical component, the logical network component, the people and the cyber identities.

- *Physical level*
  - the geographical component
  - physical network component

- *Logical level*
  - the logical network component
- *Social level*
  - interfaces
  - cyber identities.

The physical layer comprises the geographical component and the physical component of the networks. The geographic component refers to the physical location of the basic elements of the physical components of the networks. The physical network component consists of hardware and infrastructures to support their physical networks and connectors (cables, routers, servers, computers, etc.).

The logical level consists of the logical component of the networks, these are logical connections that exist between the nodes of the networks, a node being any device that is connected to the communications network and IT systems.

The social layer is composed of people and cyber identities. The *"people"* component is made up of people interacting in cyberspace. The relationship between humans and cyber identities can be from 1 to n or from n to 1, which means that a person may have one or more cyber identities and a cybernetic identity can be used by one or more people. These cyber identities can be real or false, allowing the user to enjoy anonymity and making it difficult to track the criminal behaviour that takes place in cyberspace. The cyber identities consist of, among other things, email accounts, network user accounts and social media profiles etc.

VULNERABILITIES AND THREATS FROM THE VIRTUAL SPACE VS. SECURITY ARCHITECTURES AT DIFFERENT LEVELS

According to the statistics provided by *Cisco's Visual Networking Index* and other cyberspace companies, cyberattacks are on the rise, and are becoming increasingly sophisticated. Experts are primarily concerned with the increasing complexity of cyberattacks, known as advanced persistent threats. In these types of attacks, hackers combine different ways of attacking and infiltrate companies and projects networks to steal proprietary information, stop production lines, or worse case redirect transactions. Techniques used by hackers are extremely varied. But they have a common feature: they cannot be detected by *"normal"* security features, such as antivirus programs and/or scanners. Understanding the anatomy of a cyberattack is an essential condition for understanding the threats created by virtual space, which actors can be involved, where and how these threats will unfold. A fundamental distinction in cyberspace has to be made between vulnerabilities and threats. A vulnerability is a condition for the emergence of a cyber threat – for example – an email account protected by a very simple password, such as *"123".* A threat is a combination of such a vulnerability, with an actor and motivation.

For example, a cyber killer may want to connect to an email account to get bank details or other benefits[4]. Different types of vulnerabilities can lead to various types of threats. The first and most obvious vulnerability is people: as in the previous example, a weak password, weak IT knowledge, or too much confidence in a system leads to ongoing vulnerabilities. The other type of vulnerability is computer-related. As computers run on complex and long lines of code, it is likely that an error exists at one point in one of the codes.

Analysis of the critical infrastructure security dialogue

Different perceptions about the role and strength of the internet are an important factor behind the lack of an early warning mechanism in the field of cyber security. The only attempt at the international level was the *Budapest Convention*, or the *Convention on Cybercrime*. This treaty addresses important cybercrime issues, but does not address other additional issues such as the early warning mechanism that could help eliminate the anonymity of cybercriminals in cyberspace.

The *Budapest Convention* is signed by fifty states, but it does not have the necessary support from Russia and China, which are non-signatory states, because of their domestic efforts to censure their populations and hence resistance to international efforts. The UN-level debate on cyber security has capitalised on a lot of talks but has not produced any concrete results. The first mention of cyberspace took place in the 1998 General Assembly and the first GEG was convened in 2004. It is important to note that this initial meeting of the GEG was non-profitable, and in the end, experts were unable to produce any resolution.

Currently, the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) are at the forefront of UN initiatives in the cyber arena. UNODC focuses on the cyber space that relates to their main areas of authority, namely on-line organised crime and child abuse. The ITU sets international standards in a number of areas, ranging from expanding Internet access to providing Key Telecommunications Union *("Key Areas of Action")*[5].

Perhaps the most complete attempt to take into account the international legal implications of cyberattacks is the Tallinn Manual on international law applicable to cyberwar. Developed over a period of three years by twenty international legal scholars, the manual sets out ninety-five *"rules"* covering the legal implications of cyberwar on state responsibilities and sovereignty. These rules attempt to identify under what situations existing international law can be applied directly to the cybernetic domain. In addition to disagreement over the value of the Internet,

[4] P.W. Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, Oxford, UK. Copyright 2014.

[5] http://www.itu.int/en/action/Pages/default.aspx

the development of international law is hampered by the speed of technological progress. Legislation development, especially at international level, is a long process that is often overcome by these technological changes. For example, the emergence and proliferation of smart phones has changed the landscape of threats and vulnerabilities and has therefore modified the considerations of UN resolutions and international conventions[6].

Levels

In order to conceptualise cybersecurity and develop protection policies, we need to divide the virtual space into categories where vulnerabilities are most likely to be present. An opportunity to establish a framework for understanding the concept of cyber security would be to analyse cyberspace at different levels, each level indicating the consequences for different cyber-infrastructure disruptions. The consequences of cyber incidents and corresponding response mechanisms are quite different at global, regional and national levels than those at the level of social structures, economic sectors, or individuals. But all of these levels are tightly connected to virtual space, and any effective response mechanism must address them all at the same time.

❖ *Global and regional level*

The most serious and profound consequences are caused by global and regional information infrastructure disruptions. At global and regional level, international incidents response mechanisms and formal cooperation networks should be made up of governments, international organisations, ICT stakeholders in order to ensure incident management capabilities in case of any interruption. Therefore, the international dimension and the practical prevention mechanisms in the field of cybersecurity cannot be underestimated.

At international level, there are several major players in the international cyber battlefield, Russia, the United States, China, which have their own strategy on cyberspace. For example, the United States – *The International Cyberspace Strategy* (2011), called *"Prosperity, Security, and Openness in an Interconnected World"*, strategically addresses the world of cyberspace as *"a world we depend on every day. This has made us more interconnected than ever in the history of mankind. The foundation of international policy on the United States' cyberspace is the belief that network technologies have huge potential for our nation and the world. With regard to adaptation to meet these new challenges, we will pursue a policy*

[6] Tallin Manual, 2009.

of the international cyber space by encouraging innovation that guides our economy and improves our lives here and abroad", President Barack Obama, 29 May 2009.

As far as the European Union policy is concerned, the European Commission launched the *EU Cyber Security Strategy covering the Internal Market, Justice and Home Affairs*, as well as approaches to cyberspace foreign policy in 2013. The strategy is accompanied by a legislative proposal to strengthen the security of the EU's information systems.

The Strategy sets out clearly the priorities of EU policy in the international virtual space:

- freedom and openness: the strategy presents the vision and principles on the application of the fundamental values of the EU as well as fundamental rights in cyberspace;
- the laws and fundamental values of the EU apply equally in the virtual world as in the physical world: responsibility for a safer cyberspace lies with all actors in the information society worldwide, starting with citizens and ending with governments;
- developing cybersecurity capabilities: The EU is engaging with international partners and organisations, the private sector and civil society to support the strengthening of capacities worldwide in third countries. This includes improving access to information and an open Internet as well as preventing cyber threats;
- promoting international cooperation in the virtual space: keeping open, free and secure cyberspace is a global challenge to which the EU is working together with international organisations and relevant partners, the private sector and civil society.

The EU's cybersecurity strategy combines expertise in strategic analysis, information, training, prevention, with the aim of gaining insight and understanding of the thinking and action of high-tech offenders, delinquents and fraud in cyberspace. This understanding is then shared to allow more effective targeting of law enforcement operations, to influence and inform policy and legislation changes, to invite public-private partnerships to cooperation and, most importantly, to advise citizens and businesses/projects on how to better protect themselves in the digital world[7].

The security strategy in the EU's cyber environment is an essential component of the global strategy, involving all member states, major Internet providers, critical infrastructure operators (e.g. e-Commerce and social networking platforms) energy,

[7] https://www.europol.europa.eu/ec3

transport, health and the banking sector, to ensure a secure and trustworthy digital environment across the EU. The measures envisaged include the following:

- member states must adopt a network and information security strategy and designate a competent national authority with adequate financial and human resources to prevent, manage and respond to risks and incidents;
- operators of critical infrastructures in certain sectors (financial services, transport, energy, health), information society service facilitators (especially online stores, trading platforms, Internet payment, search engines, social networks) and public administrations to adopt risk management practices and to report major security incidents on their core services;
- a cooperation mechanism should be created between member states and the European Commission to share early risk and incident warnings through secure infrastructure, cooperate and organise regular assessments[8].

While the European IT insurance market is still under development, many companies in the United States already have liability policies to cover data loss. This is due to the fact that US companies are compelled to inform their clients about breaches of security. The introduction of similar regulations is currently being discussed in the EU member states.

❖ *National level*

Increasing cyberspace as a field of human activity is probably one of the most important developments in the history of the world. Cyberspace already has a direct impact on every aspect of human existence, including economic, social, cultural and political developments, and the pace of change is not likely to stop too soon.

However, socio-political responses to questions raised by cyberspace growth often remain significantly behind the technology exchange rate. One of the areas most prompted by this evolution is that of *"national security"*. *"Cyber-races"* exist in different corners of the world and this is a fact known to EU countries as well as to organized crime groups and terrorism. Fortunately, a growing number of countries in Europe have a National Security Strategy for the cybernetic environment as a key feature of policy, helping them address risks that have the potential to undermine the realization of economic and social benefits in cyberspace.

Eighteen member states of the European Union have already published *Cybernetics National Security*, and some of them are at the second revision, but they are still in an increasingly difficult situation because using cyberspace requires the principle of total asymmetry if critical public and private information systems are being attacked by IT professionals with advanced IT tools. If simple citizens

[8] https://www.europol.europa.eu/ec3.

and business owners do not trust cyber security, it is obvious why they could avoid participating in online activities, thus inhibiting cyberspace development opportunities. The *European Network and Information Security Agency (ENISA)* has published all the documents that regulate national cyber security strategies in the EU, but also in the world, which are available to the public.

- Austria – *Austrian Cyber Security Strategy* (2013);
- Belgium – *Belgium's Cyber Security Strategy* (2014);
- Czech Republic – *Cyber Security Strategy of the Czech Republic for the period 2015-2020*;
- Cyprus – *Cyber Security Strategy of the Republic of Cyprus* (2013);
- Denmark – *National Strategy for Cyber Space and Information Security* (2011);
- Estonia – *Cyber Security Strategy* (2014);
- Finland – *Cyber Security Strategy* (2013);
- France – *Defence and Security of Information Systems* (2011);
- Italy – *National Strategic Framework for Cyber Security* (2013);
- Germany – *Cyber Security Strategy for Germany* (2011);
- Hungary – *Cyber Security Strategy* (2013);
- Latvia – *Cyber Security Strategy* (2014);
- Lithuania – *Program for the development of electronic information security* (2013);
- Poland – *Cyber-friendly policy* (2013);
- Romania – *Cyber Security Strategy* (2011);
- Slovak Republic – *National Strategy for Information Security* (2008);
- Spain – *Cyber Security Strategy* (2013);
- United Kingdom – *Cyber Security Strategy of the United Kingdom* (2011).

In the field of cybersecurity, where the vast majority of information infrastructure belongs to the private sector in EU countries, new crisis management frameworks and public-private partnerships should be developed as a response to a new threat landscape. Many experts, especially from the United States and the EU, are currently discussing whether to launch a new international treaty on cyberwar. Unfortunately, this remains a theoretical exercise. EU countries need to constantly update national cyber strategies and develop e-information infrastructures run by an educated workforce. EU governments could also benefit from the development of an international exchange of information and early warning and assistance mechanisms in cooperation with our strategic partners, the US and NATO, for rapid response in times of crisis, and the establishment of a consultation with other countries.

Romania's cyber security strategy – a brief overview

In line with the European Cyber Security Directive, Romania assumes the role of coordinator of activities at national level to ensure cyber security in line with EU and NATO measures. The issue of cyber security has become a priority for Romania in its relationship with the EU and NATO, which involves regulatory measures needed to develop cyber defence mechanisms. The goal of Romania's cyber security strategy is to define and maintain a secure, highly secure and trustworthy virtual environment based on cybernetic national infrastructure, which is an important support for national security and good governance, maximising benefits citizens, the business environment and the Romanian society as a whole. The Romanian Cyber Security Strategy sets out the objectives, principles and main directions of action for understanding, preventing and counteracting threats, vulnerabilities and cyber security risks and promoting Romania's interests. Increasing cybercrime capacity at national, European and international level involves, among others:

- increasing the level of cooperation and coordination between the cybercrime units, other authorities and experts in the European Union;
- developing a coherent EU regulatory framework for fighting cybercrime, in coordination with member states and European and international authorities in the field;
- increasing awareness of the costs and the dangers of cybercrime.
- the main objectives of public-private cooperation on cyber security issues.

In this context, Romania recognises the existence of such a threat and supports a common, integrated and coordinated approach to both NATO and the EU in order to provide a timely response to cyberattacks. Co-operation for development between the public and private environments in order to ensure cyber security is a priority of action within the international bodies or alliances to which Romania is a party, since the cybernetic space brings together both cyber-owned and managed infrastructures and private entities:

- changing information on threats, vulnerabilities and risks;
- developing capabilities for rapid alert and response to cyber incidents and attacks;
- development of common security exercises in cyberspace;
- development of educational and research programmes;
- developing security culture;
- Joint reaction in case of major cyberattacks.

Achieving goals involves collaboration between the public and private sectors, including prevention, awareness and promotion of opportunities in cyberspace.

Last year, the bill on cybersecurity, named in the media Big Brother as part of the national cyberstrategy, was approved by the Romanian Parliament, but it was declared unconstitutional entirely in accordance with Decision no. 17/2015 of the Romanian Constitutional Court.

CONCLUSIONS

We need to integrate national security strategies into an early warning mechanism for advanced cyber threats.

There is a tremendous interest in developing proactive methods and predictive cyber defence capabilities, anticipating future attack strategies to allow for early identification of emerging contentious situations, accurate detection or forecasting of potential *"viral"* ideas or behaviours.

The requirement for international cooperation to provide an early warning of cyberattacks on common infrastructures has been recognised by decision-makers in EU governments and corporate policy in Europe. Although there are ad hoc warning mechanisms (e.g. CERT), Europe needs to examine best practice in this area to create early warning mechanisms that can add value at national and transnational levels. All of the above-mentioned national EU mechanisms are not sufficient for large-scale cybercrime and the fight against organised international cybercrime. Developing an international and regional exchange of information and early warning mechanisms and cybersecurity consultations are long-term challenges for governments and industrial projects in the 21st century. New practices based on an understanding of the phases of an attack, ongoing threat monitoring, rapid detection of attacks and their resolution are mandatory. The European Council identified the *"early warning"* as an urgent requirement in the eEurope Action Plan. The requirement for international cooperation to provide early warning in case of malicious attacks on critical infrastructures has already been recognised by EU governments' decision makers who have noted that such a warning requires new paradigms of information exchange between the public sector and private and beyond national borders.

Parallel developments in national security provide us with a number of models for many highly alert and alert construction levels that link the threat detection to proactive response measures. However, integrated alert, alert and response architectures already operate in the United States and the development of a wider EU approach to prevention and response to threats that have the potential to undermine the reliability of infrastructures is becoming increasingly urgent. The Early Warning concept has become fundamental in ensuring and protecting information and must be clearly differentiated from the concept of threat assessment, which has been detailed above. The Early Warning System was first

used by military security agencies to identify threats/risks to national security. Nowadays, in addition to military agencies and organizations, the concept of early warning system is used with great success in operations for the stability of the international security environment (UN, OSCE, etc.), environmental protection, natural disaster prediction, the control of epidemics, the prediction of sudden changes in the economic environment, etc.

Below there are some early successful early warning models that are not specifically focused on cyber threats, but they provide useful insights into early warning methodologies:

- generic early warning and information exchange models:
- government-citizen travel warnings;
- government-citizen warnings of natural disasters or bad weather;
- government-citizen warnings civil defence (air raid) and terrorism;
- weather forecasting services;
- forecasting services for scholarships;
- political risk forecasting services.

There are also examples of early-warning commercial vendors: Paraprotect, Internet Security Systems ISS, and i-Defense, Global Integrity, RealSecure, SAFEsuite, LogiKeep, Riptech.

BIBLIOGRAPHY

1. ***, *Germany Cyber Strategy, National Strategy for Critical Infrastructure Protection*, Ministry of Interior, p. 14. 2009.
2. ***, *'Study Group 17 at a Glance',* International Telecommunications Union, url: http://www.itu.int/en/ITU-T/about/groups/Pages/sg17.
3. CISCO, *Visual Networking Index*, 2014.
4. European Commission, *Preparedness and Consequence Management in the Fight against Terrorism. Communication from the Commission to the Council and the European Parliament*, Brussels, COM, 701, available at *http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0701:FIN:EN:PDF*, 2004.
5. European Commission, *Critical Infrastructure Protection in the Fight against Terrorism. Communication from the Commission to the Council and the European Parliament*, COM, 702, available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:NOT, 2004.
6. European Union, *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cybersapce*, 2013.
7. A. Gheorghe, *Infrastructuri critice. Riscuri şi vulnerabilităţi în contextul european*, in *Impact Strategic* no. 1/2005, Editura Universităţii Naţionale de Apărare *"Carol I",* pp. 150-152.

8. Microsoft, *CIP Principles: Critical Connections, Microsoft Global Security Strategy and Diplomacy*, p. 4, available at *http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8026*, 2009.
9. Microsoft, *Critical Infrastructure Protection Concepts and Continuum, Microsoft Global Security Strategy and Diplomacy*, p. 10, available at *http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=325*, 2009.
10. US National Institute of Standards and Technologies, U.S. Department of Commerce, http:csrc.nist.gov/publications.
11. M. Rizea et al, *Infrastructuri critice*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2010.
12. P.W. Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, Oxford, UK. Copyright 2014.
13. World Meteorological Organisation, *Global Assessment Report on Disaster Reduction: Thematic Progress Review Sub-Component on Early Warning Systems*, 2009.
14. World Economic Forum, *World Economic Forum Report*, 2013.
15. https://www.europol.europa.eu/ec3.
16. http://www.worldcat.org/identities/lccn-no2012150259.
17. Symantec's 2014 Internet Security Threat Report.
18. http://www.itu.int/en/action/Pages/default.aspx.
19. http://www.microsoft.com/security/cipp/default.aspx

CONSEQUENCE MANAGEMENT, CRITICAL INFRASTRUCTURES AND THE ART OF MILITARY OPERATIONAL PLANNING

Daniel ROMAN, PhD

Senior Lecturer, the Faculty of Command and Staff,
"Carol I" National Defence University, Bucharest

The complexity of the essential areas of life at a societal level and the difficulty of identifying the elements threatening them are the main issues that the contemporary societies have to face, regardless of their economic development. Thus, the dynamics of changes in the defining environments of a society set a specific rhythm of the societal activities that are interdependent and determine a network behaviour specific to all the actors involved. According to the importance of the outcome of the totality of actions in these fields, a certain extrapolation on the future results, namely a possibility of expressing those scientifically argued predictions, such as the ones belonging to the field of consequence management. The notions of peace and security at the societal level are directly influenced by the complexity of the cooperation and the coordination between the pillar factors: political/diplomatic, military, economic, social, infrastructural, informational and environmental, with major implications on the population and the space, calculated within a specific time frame. Taking advantages of the weaknesses and capitalising on the possible occurrence of a risk or a major impact negative event can degenerate under certain conditions to border situations, crisis, armed military conflict or even a hybrid war. The art of the operational planning in the military field can be considered the reference point in the development of the societal threat scenarios, according to the established level of particularisation, be it tactical, operational or strategic. The joined approach to the operational planning on several levels and on societal domains of a crisis or hybrid war occurrence can be one of the solutions for solving the standstill situations or the societal throw-back. Therefore, we considered it was necessary to clarify those theoretical aspects regarding the possible bi-univocal conceptual undertaking of the operational art of planning the military operations to other fields such as consequence management and critical infrastructure protection.

Keywords: societal domains, consequence management, operational planning, military operations, critical infrastructures, crisis, hybrid war.

ON THE CONSEQUENCE MANAGEMENT IN THE SOCIETAL CONTEXT

The profound transformations in the technological – industrial sector specific to the contemporary societies have generated a series of important changes and mutations in all areas of daily life. The digitisation of information and the speed of processing it contribute to decoding the ways of societal phenomena occurrence. In order to understand the expressions containing the notion of *"societal"*, the term must be defined, so that any reference to it clearly expresses the situation it refers to. The term *"societal"* is defined as the context or the operational environment of manifestation of all the actors directly or indirectly involved in a delimited space belonging to a community. Employing the power tools at the community level – as a subject of analysis, be it a state or an alliance, is the manifestation of all the phenomena related to: population, territory and essential elements of life (vital products and services/critical infrastructures) contained within a certain precisely established historical time span. Understanding the ways in which the societal phenomena occur can generate the possibility of extrapolation on the future of a certain community, namely an identification of the possible consequences on the latter and implicitly the achievement of a consequence management based on case studies, or on designed scenarios.

The phrase *"consequence management"* appears in 1995 in the US DoD security lexicon, with the promulgation of the Presidential Directive no. 39 (PDD 39)[1], a situation generated by the events of the sarin gas terrorist attack in the Tokyo subway (12 dead and hundreds of injured severely intoxicated with sarin) as well as other events leading to the development of US counterterrorism policy guidelines[2]. The development of the consequence management is based on the perishable nature of the essential products and services of the society as a whole. This *"perishable nature"* can be generated by the situations achieved by different forms of terrorist threats or as a result of natural disasters and catastrophes or industrial accidents (Chernobyl – 1986) and, last but not least, as possible direct or indirect results of the military conflicts, crisis situations or consequences of the hybrid warfare. Thus, Presidential Directive no. 39, expressed in the societal

[1] Chris Seiple, *Another Perspective on the Domestic Role of the Military in Consequence Management*, p. 1, available at http://wearcam.org/decon/victims_videotaped_trough_decon_line.htm retrieved on 29.07.2019.
[2] http://www.ojp.gov/odp/docs/pdd39.html retrieved on 29.07.2019.

context, establishes consequence management as a method designed to fulfil a series of requirements for the public protection, safety and welfare. In the same area of reference of the consequence management there are the restoration of the essential government services and the emergency aid of the affected areas, the companies and the citizens affected by the consequences of an emergency situation, terrorist attack/industrial accident where chemical, biological, nuclear and/or highly explosive substances have been released[3]. In the same direction of understanding the consequence management, NATO brings a new vision to the concept, which essentially refers to actual reactive measures to mitigate/remove the destructive effects following a terrorist attack, incident or natural disaster[4]. This fact opens new horizons for the planning process, the establishment of inter-institutional and interdepartmental agreements that will immediately apply the developed solutions before the occurrence of a critical situation[5]. On the same trend of the legislative measures to counter the risks following terrorist attacks with weapons of mass destruction, the European Union issues Decision 124/2007. According to this document, the concept of consequence management is established, referring to *"coordinating the measures taken to respond to reduce the impact of the effects of the security incidents, especially those resulting from terrorist attacks, in order to ensure a homogeneous coordination of crisis management and of security actions"*[6].

As a result of the legislative efforts within the most representative forums, there is an integrative attitude at the conceptual level regarding positioning the consequence management to the other forms of management, such as crisis/crisis response management or emergency situations management. Thus, we find out that crisis/crisis response management is in the range of the solutions specific to those situations in which the initiators of dangerous acts of terrorism could be discovered before the onset of an attack, such as one with weapons of mass destruction[7]. On the other hand, the consequence management is placed in this category due to the description of the ways, methods and means designed for reducing in the short and long term the physical, socio-economic and psychological effects of the attacks with weapons of mass destruction[8]. The distinct advantage of the consequence management is that before the terrorist attack with NBCWMD (nuclear, bacteriological, chemical and highly explosive weapons of mass destruction) or the occurrence of the major impact negative event – SMINE

[3] http://www.dtic.mil/doctrine/jel/doddict/data/c/01195.html retrieved on 23.07.2019.
[4] Constantin Moştoflei, Grigore Alexandrescu, Cristina Bogzeanu, *Managementul consecinţelor*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2009, pp. 12-30.
[5] http://www.nato-otan.org/issues/terorism/practice05.html retrieved on 23.07.2019.
[6] Council Decision 2007/124/EC, Euratom of 12.02.2007, Art. 2, par. b.
[7] Chris Seiple, *op. cit.*, p. 2.
[8] *Ibid*.

(under CBRN incidence), the means to coordinate the appropriate assets, all the training activities before the occurrence of negative situation are described. The prevention and intervention package includes the surveillance of the target area, the assessment of the capabilities of the intervention and the medical units, the check up of the quantities, quality and dislocation of the service supply points for procuring the necessary materials for the intervention, the decontamination of the victims or the affected facilities. In the same context but under an integrated aspect, the situation of the responsibilities regarding the management of a crisis situation can be interpreted as a network of interdependencies on societal domains, as shown in *figure 1*.

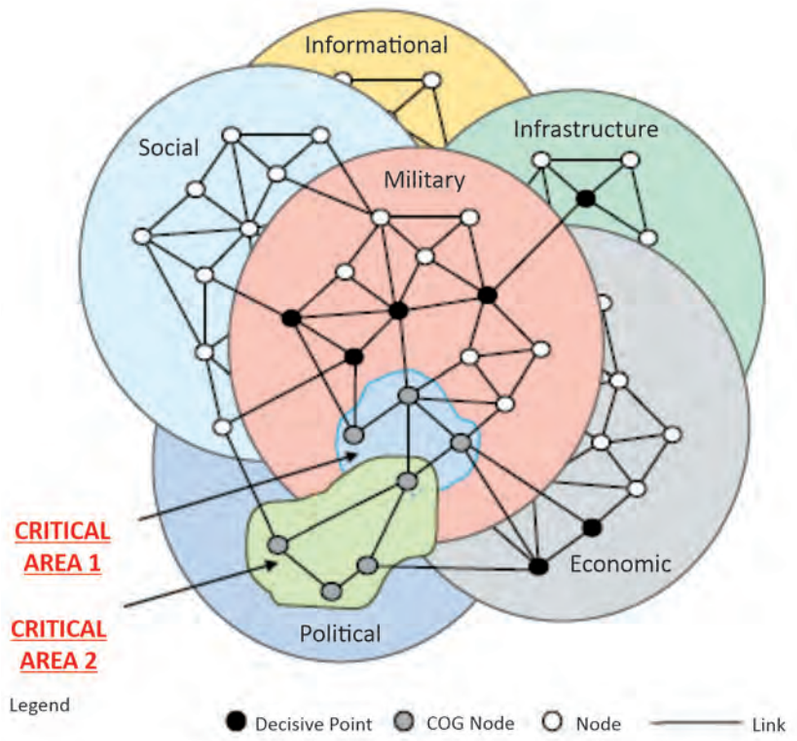


Figure 1: Graphical representation of the network interdependencies on societal domains[9]

This fact, based on the mutual determinations and conditions of the societal domains of a territory with a certain population, generates the possibility of designing and developing an integrated consequence management. Thus, the general

[9] Cristian Dincovici et al, *Manualul privind pregătirea întrunită de informaţii a mediului operaţional*, Editura Militară, Bucureşti, 2014, p. 89.

features of the structures involved or connected (according to the network model) can be identified for the specific achievement of the consequence management. Depending on the situation, the central role is played by that actor specialised in managing a certain type of crisis that can be: political, economic, social, military etc., while the other actors will contribute to diminishing the negative effects according to their skills. In this regard, the *"NATO military concept for fighting terrorism"*[10] specifies that each member state takes action primarily as a measure to reduce the consequences and the effects of a terrorist act. From a joint point of view, NATO militarily supports such a critical situation from the prevention phase by establishing a cell specialised on the coordination between NATO and a potential affected state. For this, different phases are established for the intervention, namely the planning, the early warning and the timely deployment of specialised CBRN forces, IT engineers, search and rescue specialists for the identification and the evacuation of personnel or dangerous materials etc.

The novelty regarding the explanation of a complex crisis situation and the method of intervention according to the consequence management is given based on the operationalisation of the notion of *"societal domain"*. This fact includes the possibility that an incident specific to a societal domain, may have small implications or effects, even insignificant in the field in which it occurred, but serious, sometimes critical and irreversible consequences in another societal domain. For argumentative purposes, we exemplify by *"the Colectiv case"* on 30 October 2015 in Bucharest. Without going into the *"technical details"* of the negative event, it can be classified as a negative event with major societal impact, due to the consequences it has generated. Following the large-scale street protests following the fire, the prime minister, along with the government and the mayor of the sector of the affected area resigned[11]. This shows that, from a societal point of view, the consequence management activities have not been synchronised to prevent the extension of the event belonging to a certain societal domain to another societal domain. The influences between the societal domains in terms of their network connections, political/diplomatic, military, economic, social, infrastructural, informational and environmental, can have major implications on the population and on the territory, and they can be predicted on a certain time span. This leads to the assertion that the ways of calculating or interpreting the consequences of a negative event in a particular societal domain may have a greater impact and far more serious implications in the other societal domains.

[10] http://www.nato.int/ims/docu/terrorism.htm.

[11] https://www.mediafax.ro/politic/colectiv-guvernul-ponta-primul-executiv-rasturnat-de-vocea-strazii-de-la-mineriade-incoace-cum-au-incercat-unii-sa-mistifice-tragedia-16798310.

A first hypothesis can be expressed regarding the *"specific behaviour according to the societal domains"* where those negative events with major societal impact can occur. This fact shows that the network connections established between the societal domains determine a particular geometry of the consequences when one or more negative events occur. In other words, based on the established hypothesis, there is a possibility that one of the societal domains, in relation to the network connections that it has with the other societal domains, may become the weak point of a state or alliance. From the point of view of the art of the operational planning of military actions, this affected domain which has the potential to have a major societal impact becomes the *"center of gravity"* of the state that is undergoing a certain crisis situation. If the negative event with a major societal impact affects a vital service or product which is highly necessary and specific to the critical infrastructures, we can express another hypothesis[12]. The *"decoding"* from a societal point of view of a country, of the state of normality and of a critical or crisis situation, can be achieved by simultaneously overlapping three of the domains designated as having specific societal content: *the consequence management*, *the critical infrastructures* and *the art of the operational planning of the military actions* (*AOPMA*). Following the overlapping of the three fields of interpretation and reflection on the actual situation, it is possible to foresee that possible future or, in other words, several futures may be envisaged which could occur when certain conditions or circumstances are met. The operationalisation of the phrase *actual situation* in the societal context distinguishes between several possibilities of expressing *the reality*. Thus, several *societal realities* are distinguished, which are directly related to the social domains in which they are expressed: the reality of the political situation, the reality of the economic situation, the reality of the military situation, the reality of the social situation, etc. All these societal realities are ways of decoding the same society but under several aspects, depending on the affected societal domain or the power of the connections the domain has with the other domains, according to a network connection scheme, shown in *figure 1*. The gravity of a situation in which a society can find itself (the population of a state or of a certain territory, regardless of the number of states involved) can be measured through the intersection area of the consequence management, critical infrastructures and the art of the operational planning of the military actions. We will exemplify by referring to the *"Tallinn case"*, 2007 when following certain *"coincidences"*, in the very day that the Soviet Soldier's Monument was moved from the centre

[12] *European Council Directive 2008/114 of 8 December 2008 on Identifying and Designating the European Critical Infrastructures and Assessing the Requirements for their Protection*, Brussels, 2008, http://ccpic.mai.gov.ro/docs/directiva114_RO.pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF, retrieved on 07.09.2019.

of the Estonian capital, unprecedented cyberattacks were launched on the public institutions, the banks and the media. The causes that triggered the cyberattacks can be considered to have a social nature, but the effects of the attacks in this case have exceeded the social sphere towards at least the economic and the state security domains[13]. Assessing the consequences of such complex situations is difficult to achieve due to the network connectivity of all the societal domains[14]. Thus, the geometry of societal network connectivity is difficult to draw from a static point of view, this being possible only in the dynamics of the events, which is achievable by means of the theoretical apparatus specific to the art of the operational planning of the military actions.

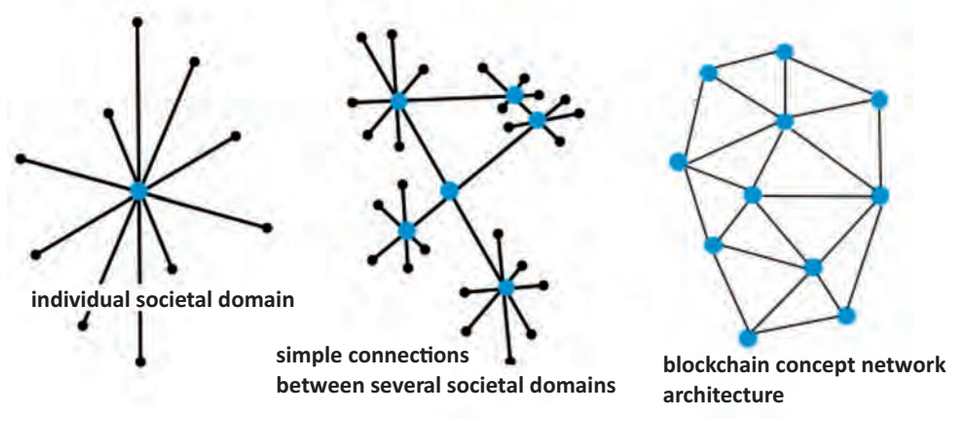


Figure 2: Graphical representations of several network models, where the distributed collaborative work network can be geometrically compared with the other network models, namely the centralised and the unidirectional ones[15]

The art of the operational planning of the military actions is based on anticipating and planning critical events due to the possibility of estimating the capabilities of a confrontation between two or more opponents. Determining the opponent's centre of gravity, respectively the means and the methods of engaging him are paramount for achieving the desired end state. Thus, the operational design of the art of the operational planning can be considered to be a starting point in explaining the fact that a negative event with a major impact on one or more societal domains can be anticipated and countered using the theoretical support adapted from the planning of the military actions.

[13] Petrişor Pătraşcu, *Cybernetic Actions Critical Infrastructures in the Military Field*, Bulletin of *"Carol I"* National Defence University, no. 1/2019, București, 2019, p. 40.
[14] Stephen P. Robbins, *Organizational Theory: Structure, Design, and Applications*, Prentice Hall, New Jersey, 1990.
[15] https://fr.coinnewstelegraph.com/an-etf-to-capitalize-on-the-disruptive-blockchain-technology-png/, retrieved on 16.09.2019.

THEORY OF THE OPERATIONAL PLANNING OF THE MILITARY ACTIONS IN CRITICAL INFRASTRUCTURE PROTECTION

The imbalances that can occur at the societal level in certain areas with centralised and decentralised architecture can be analysed individually in terms of the action of the destructive factors, which means that action plans can be drawn up to increase the post-event resilience. In this context, the social network model can be explained in at least two ways. A first variant refers to the way of establishing the network connections between the societal domains as in *figure 2*, where the role of the nodes and the nature of the interactions between them are important. In an advanced geometric form, based on the links between the societal domains, that collaborative working network or a blockchain institutional network can be achieved. In this variant, the states of normality that have a strong institutional character at the societal level can be expressed and described. The second variant expresses the state of abnormality in which the societal domains are affected by internal or external destructive factors. The damages, the partial or permanent destruction of one or more societal domains implies the reconfiguration of the societal network based on *"other rules"*, possibly non-institutional. We chose to use the phrase *"other rules"* to stay in the area of control of the situation, which may be crisis, military conflict or hybrid warfare. The triggering factor of the state of societal abnormality may be of different nature depending on the affected societal domain: political/diplomatic, military, economic, social, infrastructural, informational and environmental. The most important aspect in delimiting the affected social domain is to identify the type of the major impact negative event that can be: a deep economic crisis, a military conflict, a natural disaster or a large industrial accident. In order to identify the direction of the propagation of the destructive wave having a societal impact, the operational design of the events can be developed, where the links between the network societal domains starting from the affected area. Chronologically with the events and based on the links with the other domains, the effects are identified and subsequently, the consequences that can result from the propagation of the shock wave are anticipated.

The propagation of the shock wave in the area of the societal domains, as a result of the negative major impact event occurrence, can be considered as a sequence of events similar to the unfolding of a military conflict transposed in the operational design of the art of the operational planning. Starting from this, the identification of the geometric form in which the social network is transformed is conditioned by the nature of the links between the societal nodes, the role of the societal nodes and the resilience of each societal node. Considering the manifestation of the destructive

factor on a societal domain as actions of an enemy/aggressor specific to the situation of military conflict, the dynamics of the events affecting the domain can fall under the art of the operational planning of the actions counteracting the destructive factor. The applicability of such a theoretical approach results from transposing the affected societal domain in the area of critical infrastructure protection (CIP).

Providing the essential goods and services, due to the vital importance they have for the society, we chose to exemplify the specific societal domain as a critical infrastructure. The theoretical apparatus and the legal basis for the critical infrastructure protection are stipulated in specific documents as the *Operator's security plan (OSP)*[16]. Through its content, the operator's security plan provides the theoretical and practical background for achieving the desired end state, *the critical infrastructure protection*. The analyses led to the delimitation of the societal domains into 12 sectors of the national critical infrastructures. Due to the specificity of each critical infrastructure sector, the methodology of achieving the OSP mainly refers to the general aspects regarding the approach of the notions of safety and security in operation, the conduct of the risk management and the means of intervention on the objective in case of occurrence of an identified risk. A first observation consists in the fact that the individual approach of the critical infrastructure in question through OSP can be framed from a societal point of view within an individual geometric form or made by simple network links between the societal domains, respectively between the designated critical infrastructure sectors. This fact, based on the OSP implies at most the calculation of the possible critical situations for each critical infrastructure and the application of the sector criteria. The possibility of a major societal impact negative event is covered by the simple links of mutual dependence of the critical infrastructures based on the cross-sector criteria. Both forms of approach to the critical infrastructure protection, individually and of simple network connections, include through OSP providing the society with the essential goods and services. The results of the interactions between the societal domains without network connections, as in the examples of *"the Colectiv Case"*, 2015, Bucharest and *"the Tallinn Case"*, 2007, prove the insufficiency of the protection measures for the societal domains, respectively the critical infrastructures, supported by the OSP's theoretical background in the enacted form. In this regard, we identify specific differences between risk management and consequence management through the attitude of the responsibility factors in taking reactive actions and proactive actions towards the possibility of a negative event occurrence.

[16] *Law no. 225/2018 on Amending and Supplementing the Government Emergency Ordinance no. 98/2010 Regarding the Critical Infrastructure Identification, Designation and Protection*, Parliament of Romania, 2018.

The theory of the operational planning of the military actions has the advantage of the multidimensional approach of the engagement environment, respectively by the operational design and the possible courses of action resulting from the analyses, sets the subject in the area of a proactive attitude. The assimilation of the destructive factor in the area of critical infrastructure protection with the notion of adversary or enemy in the case of the military action planning implies a new approach of the OSP. This consists in the detailed examination of the theoretical background of the art of operational planning of the military actions in the content of the distinct chapters of the OSP. Due to the complexity of taking the theoretical background from the area of military action planning and including it in the contents of the OSP, we will return with details in further papers on this regard. To support and argue the need to implement the theoretical background from the military domain to the critical infrastructure protection domain, we will refer only to the introductory part of the reference documents, respectively, the description of the confrontation environment (development of the AOPMA estimates) and the analysis of the security environments (chapter 2 of OSP). Using the notion of *operational environment* from AOPMA in the field of CIP places the critical infrastructure or the societal environment to which we make reference in a new context, different from that of the individual approach or that in a network of simple or institutionalized connections. This new context can be described according to the systemic approach where any societal domain is a *"system of systems"* that exists in close dependence with other *"systems of systems"* and with which it directly or indirectly interacts permanently. These interactions between systems form a complex geometry of interdependent relationships, namely a blockchain network architecture, as shown in figure 2. Although, in the blockchain concept, the advantages of storing data in linked blocks are relevant and their cryptographic security is ensured, while increasing the speed of transactions, thus redefining the concept of exchange in the economic field. From a societal point of view, in a blockchain network architecture, the data carrying economic value are replaced with data on the *status parameters* of the components of each societal domain connected in the network. Thus, the relevance of those values that describe the states of system abnormality, which, depending on the origin of the negative effects, can show the direction of propagation of the shock wave formed as a result of the major societal impact negative event.

The impossibility of knowing the moment of triggering a destructive process within the societal network in a blockchain concept is decreased as a direct effect of monitoring the status parameters of each component of the connected societal domains. In other words, the intervention plans based on the estimates for each societal domain as a result of the process of solving the operational problem, respectively the plans of the operation to counteract the possible effects produced

by the destructive factors. According to the art of the operational planning of the military actions, the *estimation* is a practical, flexible tool, designed to draw logical conclusions from unclear events and situations, allowing the development of a coherent action plan[17]. The location of the possible occurrence of a negative event with major societal impact, the moment of its triggering and the direction of propagation in the societal environment are unclear events and situations, difficult to identify and to prepare for with coherent action plans. In order to solve this situation, as in the case of the operational planning of the military actions, the *specific estimating process* carried out for inaccurately defined problems, under dynamic contexts, marked by uncertainty, in high stakes situations, which must be solved under the pressure of time[18]. In this situation, it should be mentioned that the analyses and the estimates are permanent activities, established on functional elements of each societal domain, which lead to the design of the actions that must be carried out to counteract the effects of the destructive factors, to identify and minimise the consequences. In this way, sets of decisions can be formulated on what should be done and how it should be done, by answering the questions: *why, where and when, under what conditions and with what constraints*.

The process of critical infrastructure protection, namely of ensuring the functionality and the security in providing the essential goods and services at the societal level, is extremely complex and difficult to achieve. The identification of those theoretical solutions and the possibility of putting them into practice is a priority at societal level, while the adaptation of the *mechanisms specific* to the social domains with a high degree of unpredictability (the domain of the military actions) implies mainly *understanding the problem and the operational environment*.

INSTEAD OF CONCLUSION – FROM THEORY TO PRACTICE

The theoretical combination of the terms specific to distinct societal domains, such as: the domain of the military actions and the critical infrastructure protection, transposed in the perspective of the consequence management, can be one of the viable solutions for preparing the contemporary society for the occurrence of a major societal impact negative event. The geometrical architecture of the connections made between the elements specific to the societal domains, the nodes and the links between them, has two distinct possible states: the normality (acceptable) and the abnormality (unacceptable). The intermediate situations of the societal domains between the two possible states are characterised by the direction of propagation

[17] Ion Coşcodaru et al, *SMG/PF-5 Doctrina planificării operaţiilor în Armata României*, Editura Militară, Bucureşti, 2013, pp. 41-46.
[18] *Ibid*, p. 13.

and the intensity of the shock wave produced by the negative event having a major societal impact. As we have previously shown, the *consequence management* is designed to describe the ways, the methods and the means for the short and long term mitigation of the physical, socio-economic and psychological effects of the attacks with weapons of mass destruction or of another kind. Taking advantage of the theoretical apparatus specific to consequence management consists in the fact that before any incident where there is possible a SMINE occurrence, the means of coordinating the appropriate assets and the preliminary activities before the negative situation are described.

The art of the operational planning of the military actions, although it is intended exclusively for the military field, its own concepts and mechanisms regarding the implementation of the theory, covers the problems of the societal environment common to all the components of a society, most clearly expressed under an institutional relation. *Critical infrastructure protection* is the centre of gravity of any society, regardless of its economic development. Therefore, the dynamics of the transformations in the defining environments of a society imposes a specific rhythm of the societal activities that are interdependent and that determine a specific network behaviour of all the actors involved. Depending on the importance of the outcome of the sum of actions in these fields, a certain extrapolation on the future results, that is a possibility to express those scientifically argued predictions. The theoretical operationalization of the notions of societal *normality* and *abnormality* implies the existence and the permanent updating of the databases, as well as the continuous monitoring of the values of the status parameters that define each societal domain. Following the analysis of the dynamics of the values of the status parameters specific to each societal domain, predictions about their future can be made and implicitly scenarios regarding the behaviour of the destructive factors that may act in this context.

Similar to the risk management, specific to OSP in the critical infrastructure protection, establishing the documentary databases and permanently updating them with the new situations generated by the negative events are essential for expressing the hypotheses on the situations, respectively the estimates whose importance has been mentioned. In this context, it is likely that the evolution on the theoretical and practical level regarding the mechanisms of the societal domains protection will be directly influenced by the dynamics of the transformations of the operational environment. The specific approaches regarding the way of carrying out the analysis of a crisis situation, of the effects on the critical infrastructures or of a military conflict are differentiated by the way in which the problem to be solved is discussed. The correct way of expressing the problem is the first step in identifying the optimal solutions to solve it. Therefore, clarifying those theoretical aspects

of the possibility of applying bi-univocally and conceptually the operative art from the field of military action planning to the fields of consequence management and critical infrastructure protection is practically the beginning of finding the optimal solution to the societal problems.

One of the conclusions drawn from this theoretical approach is that the achievement of the individual protection of a certain societal domain is not sufficient (the representation of the individual societal domain according to figure 2). An improved situation in this regard is the conceptual development of the safety and security apparatus of one or more societal domains connected in a network of mutual determinations based on simple links between several societal domains, as in figure 2. Introducing the term of environmental operational in the technical description of the societal domains protection based on the interdependences between them is a first step in the development of a new blockchain network architecture. Related to the three distinct situations in which a societal domain can be found, as shown in *figure 2*, the art of the operational planning in the military field can be considered the reference element in the development of the societal threat scenarios, according to the established level of particularization: tactical, operational or strategic.

The societal threat scenarios are those scenarios that focus on any societal component or domain directly or indirectly affected by destructive factors capable of taking advantages of those vulnerabilities that remain unidentified at the time of the action[19]. Basically, this theoretical approach can solve the problem located outside the knowledge space specific to a particular social domain involved. This determines all the actors involved in the management of the negative event undertaking a specific network behaviour and the advantage of doing this is that the action plans for counteracting the negative effects can be written and applied in the dynamics of the development of that crisis or military conflict, which makes it *"the best along the way adjustment to the unfolding critical situation"*.

In conclusion, we are convinced that the issues of consequence management, critical infrastructure protection and art of the military operational planning remain an open topic, with new directions of approach to increase the degree of prediction about the future, prevent the occurrence of the negative major societal impact events, and in case they occur, the decision-makers will be able to act to ensure the provision of essential goods and services, to limit the consequences and to establish a real resilient character to all the societal domains.

[19] Grigore Alexandrescu; Gheorghe Văduva, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție,* Editura Universității Naționale de Apărare "Carol I", București, 2006.

BIBLIOGRAPHY

1. ***, *Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Protection of the Critical Information Infrastructures*, Brussels, 2009.
2. ***, *Council Decision 2007/124/EC*, Euratom of 12.02.2007, Art. 2, par. b.
3. ***, *European Council Directive 2008/114/EC of 8 December 2008 on Identifying and Designating the European Critical Infrastructures and Assessing the Requirements for their Protection*, Brussels, 2008.
4. ***, *Law 225/2018 on Amending and Supplementing the Government Emergency Ordinance no. 98/2010 Regarding the Critical Infrastructure Identification, Designation and Protection,* Parliament of Romania, 2018.
5. Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare *"Carol I"*, București, 2006.
6. Ion Coşcodaru et al, *S.M.G./P.F.-5 Doctrina planificării operaţiilor în Armata României*, Editura Militară, București, 2013.
7. Chris Seiple, *Another Perspective on the Domestic Role of the Military in Consequence Management*, p. 1, at http://wearcam.org/decon/victims_videotaped_trough_decon_line.htm.
8. Cristian Dincovici et al, *Manualul privind pregătirea întrunită de informaţii a mediului operațional*, Editura Militară, București, 2014.
9. Constantin Moştoflei, Grigore Alexandrescu, Cristina Bogzeanu, *Managementul consecinţelor*, Editura Universității Naționale de Apărare *"Carol I"*, București, 2009.
10. Petrişor Pătraşcu, *Cybernetic Actions Critical Infrastructures in the Military Field*, Bulletin of *"Carol I"* National Defence University, no. 1/2019, București, 2019.
11. Stephen P. Robbins, *Organizational Theory: Structure, Design, and Applications, Prentice Hall*, New Jersey, 1990.
12. https://fr.coinnewstelegraph.com/an-etf-to-capitalize-on-the-disruptive-blockchain-technology-png/
13. http://ec.europa.eu/transparency/regdoc/rep/1/2009/RO/1-2009-149-RO-F1-1.Pdf.
14. http://ccpic.mai.gov.ro/docs/directiva114_RO.pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF.
15. http://www.nato.int/ims/docu/terrorism.htm
16. https://www.mediafax.ro/politic/colectiv-guvernul-ponta-primul-executiv-rasturnat-de-vocea-strazii-de-la-mineriade-incoace-cum-au-incercat-unii-sa-mistifice-tragedia-16798310
17. http://www.ojp.gov/odp/docs/pdd39.html

STRATEGIC COMMUNICATION, PRE-STAGE OF MILITARY STRATEGY FORMULATION. COLLECTIVE IRRATIONALITY, A FACTOR IN MAKING STRATEGIC DECISIONS

Dan CRIȘAN
PhD Candidate, "Babeș-Bolyai" University, Cluj Napoca

Over the last three centuries, on a historical scale, there has been an increase in the dynamics of social transformation events, sometimes even through the development of major conflicts, as well as a progressive increase in the number of these periods of re-balancing of social systems, in a fine-tuning with the intensification of human evolution as a result of the increasingly large application of the results of the development of science. Although conflicts on the planetary scale were absent in the years after the Second World Conflagration, reducing the statistical totals regarding the number of victims associated with wars, actions of a conflictual nature, including military, from the last quarter of a century, and the increasingly clear sedimentation of a competitive multipolar world lead to the idea that these deep tectonic movements, without major effects on the plane of humanity, can be transformed into a large surface earthquake, definitive for the human nature.

The two World Wars have unequivocally shown two sides of human irrationality that pre-existed as arguments for fighting them: leaders with irrational visions and communities who believed and supported irrationally the implementation of those visions through wars. After all, there were vast communication processes that prepared and threw the world into the two disasters of the first half of the 20th century. We appreciate that, despite the exceptional level of scientific rationality and the exponential tendency of this rationality from the present stage, we find ourselves again, as humanity, in a social environment increasingly prone to the crystallisation of irrational collective options.

Society, enclosed through many of its elements in a multidimensional global network, has, more than ever, possibilities of social communication that tend towards infinity. Who should be the actors and how could they, given that there are several centres, carry out a possible process, which we define conceptually as "strategic communication", a process that will lead, in fact, to diminishing the irrationality of some leaders and/or communities and to the counter-balancing of the destructive competition of the poles of power? Does society still have the systemic immunity required to maintain its balance or to rebalance itself without reaching conflict?

Keywords: strategic communication, rational-irational, strategy, planning, public communication.

INTRODUCTION. UNDERSTANDING SOCIAL REALITY THROUGH SYSTEMATIC KNOWLEDGE

The activities of reflection on human nature, in general, and then on any topics related to this nature are both as old as the triggering of cognitive processes as well as correlated in intensity according to the degree of increase of the complexity of the processes at the level of human evolution. Existential questions to which answers have been formulated in complicated philosophical doctrines and/or scientific theories, on the one hand, and common, everyday questions related to daily life, with equally common and banal answers, on the other hand, all these stand for nothing more but the incessant struggle of man to make their life as safe as possible (**securing their offsprings** and, implicitly, the community), as long as possible (increased **life expectancy**) and as easy as possible (better **living conditions**). And, in an expression increasingly reserved at a declarative level, the human beings wanted their life to be as satisfying as possible, even full of pleasures (**hedonism**). In one of the Romanian fairy tales, the mythological character is in search of *"youth without old age and life without death"*[1]. The epic of the seeker of the utopian state reveals to us that man, regardless of status, sensed that, by overcoming some ontological obstacles, of current data, could reach a state close to the imagined status of/that they associated with providence.

The dynamics of general human evolution have led, at different stages of development, to some of the answers to the big and/or more common questions to crystallise in scientific theories with major applicative results, which in turn have proven to be true engines of *"social revolutions"* (like those used for printing, industrialisation, technologisation), with social mechanisms that overlapped the pre-existing ones and which, in our day, had the effect of **achieving the expectations established from the beginning by the human nature**: (on average) **a safer, longer and better life for the individuals of any human community**. In addition, the present, through the manifestations of the "*Fourth Industrial Revolution*"[2], including even more so, of the industries destined for entertainment, also provides contexts for the fulfilment of this subtle desire of hedonism for many of the individuals. The pursuit of individual comfort and pleasure, however, without covering the related costs through lucrative activities and, in particular, the replacement

[1] P. Ispirescu, *Basmele românilor*, Editura Polirom, 2012.
[2] D. Petre, *Noile paradigme publicitare în contextul celei de-a patra revoluții industriale*, in "*Sinteza*" Review, no. 56, ARES, Cluj-Napoca, 2018.

of costs with the access of the representatives of the *fourth industrial revolution* to the private lives[3] of individuals, lead to major repercussions in the structure of current societies and, therefore, to the recalibration of the comprehensive instrumentation of the dynamics of the current social realities.

Even though all the major transformations of the societies had their share of major conflicts, subsequently, the social systems experienced periods of rebalancing. Interestingly, the periodicity of the transformations, in a dynamic closely-knit with the development and, especially, with the historical thresholds given by the heights of the applications of science, knows an increase in its rhythmicity. These transformations are, on the scale of social progress, more frequent and denser in the last hundreds of years, in comparison to the previous millennia of human evolution. We are, in terms of the global network society of the current period of computerisation and implementation of artificial intelligence in most components of human life, in the middle of a full social revolution, with effects that we anticipate, until the next rebalancing, in terms of anxiety and even psychosocial apprehension.

However, in relation to the last three centuries, a sociological paradox or the aphorism of the *"repeating history"* can be seen: the social re-balances related to the periods of *"scientific revolutions"* have arisen as a result of major human conflicts, in the context of increasing manifestations of the collective irrationality (from labourers' conflicts to the installation of dictatorships and even wars). The degree of technological and human intellectual development, therefore of the human reason, has not implicitly led to the decrease in the appetite for the irrationality of human nature. Developed, but also emerging societies of the world know today, during a full technological revolution, manifestations of an authoritarian type, even totalitarian, upsetting the stage of the general human scientific and cultural progress through the irrational of the social decisions (including here the political, economic and military decisions) made by their leaders, but also the ones of some major parts of the societies (by voting and/or by public reactions of encouragement). In this sense, in a logic of social history, we can predict that periods of collective irrationality will continue, amplify and, most likely, degenerate into major military conflicts. However, this time, **in the search for the new social balance, due to the technological level of the societies, there is the risk of an endpoint for humanity as a whole.**

The forecasting approach presented above, the result of a brief game of the sociological imagination, is based on similar analyses that appeared in the public agora, but which have not been successful in what concerns their impact among the world's major political actors nor have they been included in the social themes

[3] *Ibid*.

of mass public communication. The events of the spectacular present do not leave room for intellectual concerns regarding tendencies of the conflict with an irreversible potential. The headliners among the communicators specialised in the area of analysis of the social system and of its different processes and dynamics are, excluding the politicians, economists, political scientists, and psychologists, a new typology of analysts of the *social esoteric space*. All of them, the ones listed above, not exhaustively, broke away from the field of sociologists, making use of it to the detriment of sociology as such. In fact, the interest shown to epistemology by the great thinkers of the social sciences, remaining rather in the field of social philosophy than in the field of the applied sociology, leads to a lack of interest in what concerns this scientific resource, given that the different audiences no longer have the levers of comprehension of the subtle and difficult-to-understand springs of the social mechanisms. In addition, the sociologists ascertain the existence of social facts "*with an eminently descriptive character*"[4], perceived as negative in the public (displayed) agora, such as, for example, exposing the ethnocentric level of one community in comparison to another, without entering, for delicacy or another reason, in the details of understanding those social facts, i.e. in the *"explanatory side of social phenomena"*[5] and, especially, in identifying mechanisms to improve them. This leads to the cession of the professional field and initiative towards other categories of interventionists. Establishing a set of good practices (operational procedures) built from the methodological baggage of sociology and engaging sociologists not only in the applied research but, especially, in providing an offer of action plans to the big social actors should be the general professional approach, in a context of public exposure, of the popularisation of the results of sociological investigations. Ultimately, **through the investigative effort of the researchers of social space and, especially, as a result of the sociological interventions/impact studies, the state of equilibrium in a society or even stages of social progress can be achieved faster and in a less difficult manner.**

THE DOUBLE MEASURE OF A COMMUNITY. ITS DEFENCE MECHANISM

Hypothetical situation: an adult person (thus fully trained, socialised) extracted from their community and located in another one will experience, beyond their (relatively) common physiological needs of humans and under similar anthropomorphic conditions, fractures of comprehension of the new social reality in which they are. Consequently, the hypothetical person we are talking

[4] P. Iluț, *Problematizări și explicitări ale cunoașterii socioumanului*, in *Psihopedagogie specială. Modele de evaluare și intervenție*, Editura Polirom, 2015.
[5] *Ibid*.

about will make a cognitive effort for resilience and operation in the new social environment and, even more difficult, will encounter an external resistance in their process of social integration. If together with the variables of *"social differences"* between the individual and their new community of integration, we also add other disturbing factors such as the anthropomorphic ones (different or even contrasting anthropological forms, such as skin colour), the gender ones (jealousy expressed by one or the other gender categories from the new community) or the power ones (imposing the will by one of the parties on the other one in the relationships that are created between them[6]) and the property ones (the appetite for the accumulation of goods by the newer member), the social conflict situation of the individual and community becomes even more complicated, a determining factor in the social dynamics of the community. But without a doubt, the social balance will re-establish itself and the community – in its new state – will continue its temporal evolution.

In the epistemological analysis of the above (simplistic) situation, we will draw the following paradigmatic considerations: the system of norms and values of a community – the operating system of the individuals; the individual – the product of their community; the state of social balance – the exhaustion/consumption of a social conflict.

1. In sociology, the system of norms and values existing in a society and the structuring effect it has on the individuals in the society are discussed with preference. In fact, this system of norms and values is much broader and subtler than the actual decryption of a set of social norms and the list of the main values of a society. The functioning rules of society – transmitted throughout the socialisation and fixation periods of the individual in the social system to which they belong – are multiple, resilient and dynamic. We suggest that this programmatic assembly of training, integration and definition of an individual towards the community should be a concept borrowed from the field of computer science: namely an "*operating system*". The analogy is not forced, given that for computer science, the operating system is defined as "*the first program loaded in the memory of the computer that remains active for the entire duration of its operation and plays the host role for the applications running on the respective equipment*"[7], a very appropriate definition to what happens to an individual during their training period, up to the adult stage. In this sense, the individual is the product realised as a result of both what they inherit (their genetic baggage – the technical characteristics) and their "*psychosocial process of transmitting-assimilating the attitudes, values, conceptions or patterns*

[6] Max Weber, *Wirtschaft und Gesellschaft*.

[7] R. Rughiniș, R. Deaconescu, G.G. Milescu, M. Bardac, *Introducere în sisteme de operare*, Editura Printech, București, 2009.

of behaviour specific to a group or community in order to form, adapt and integrate socially an individual"[8]. Obviously, based on a pre-existing operating system, the individual can still assimilate other additional data (other *programmes*) with which to operate during their life. And, similarly to a computer operating system, there is the possibility that certain applications/programmes will fail to enrol in the main system, leading to operating difficulties or even to the failure of the system as a whole. Between societies that are similar from the point of view of their social development, there are similar operating systems for the individuals that form them, with possibilities of adapting individuals from one society to another, just like between societies with very different levels of social development, the possibilities of adaptation of individuals are very difficult or not possible at all.

2. People are the products of their community of origin from the historical stage of the community in which the reference takes place. From the beginning, we exclude the infinite possibilities of the particular situations of the type "*for me it is a little different because ...*" or "*I know someone who ...*" or "*in my family, there is someone more different than ...*" etc. The exclusion of *"subjective appraisals*", which come to invalidate the flat statement, in fact, a banality resulting from the (more) systematic knowledge of social realities[9], occurs because the paradigm of the man belonging to the community of which they are part of and to their identification as an anthropological product is confirmed not only by rigorous analysis but also by the knowledge of the common-sense type.

3. A human community knows repeated conflict states and processes of restoring the social balance during its evolution. Although the evolution factor itself is precisely the conflicting nature of the individuals of the community and of the social relations in constant competition for resources between the elements of the social structure, the adoption of (temporarily) equilibrium states is the defining ontological feature of the respective community. The paradigm of social conflicts[10] explains, by identifying the centres of authority, the balance that is established in the conflictual relations between different centres – authorities.

It is easy to see from the presentation of the hypothetical situation and from the paradigmatic considerations that we have an individual with an operating system specific to a community (of origin) in their attempt to re-integrate into a community (of destination) with its own and different system of operation. As a result, there is a conflict state in the destination community and a state of cognitive effort to integrate the individual into it. By virtue of the paradigm of social conflict, in the cycle of evolution of communities, conflicts tend to appear and be resolved, restoring

[8] C. Zamfir, L. Vlăsceanu, *Dicționar de sociologie*, p. 555, Editura Babel, București, 1993.

[9] P. Iluț, *op. cit*.

[10] R. Dahrendorf, *Class and Class Conflict in Industrial Society*, University Press, Stanford, 1967.

the (temporary) balance state of the community. Thus, we can assume three courses of action in the relationship mentioned above: the individual is either assimilated by the community (1), or the community changes under the effect of the individual's force (2), or the individual leaves the community in which they entered (3).

The community and its operating system have different approaches when it comes to their own members versus any external ones. It is a game with a double measure, obviously, the favourable one being applied to its perfectly integrated and functional individuals (anthropological products of the respective community) while the unfavourable measure, one of resistance, is applied to external individuals, identified as a danger to the existence of the community in its original form. It is, moreover, a mechanism of defence of the community (sometimes brutal towards change), in a conflict that can affect it (fundamentally).

SYSTEMATIC ANALYSIS OF THE SOCIO-HUMAN REALITY – HUMAN NATURE'S DESIRE

There are two ways of approaching the previous situation and, in essence, any possible socio-human reality. From the perspective of *common knowledge* and from the one of *systematic knowledge*[11]. In both, methods will be used to understand and solve the situation, in which ordinary individuals or social investigators will use, obviously with differences of depth and scope of research in different stages of the analysis, *"assigning probabilities to events, predicting the future, evaluating hypothesis and frequency estimation"*[12] and even "*assign[ing] causes, operat[ing] with rather sophisticated inferential statistical methods, such as covariance (Kelly, 1976), generaliz[ing] and mak[ing] predictions*"[13]. Apparently, because we will see that next to the "*limits and errors detectable in the common consciousness*"[14] also stand the *"heuristics and biases"*[15] and even dogmatic thinking, including that of the scientists, which all lead to *"systematic errors"* and therefore to conclusions which are, many times, wrong.

We have, therefore, the first level of analysis, common to the two categories (ordinary individuals and social investigators), given by the easy access to the *socio-human reality* that becomes *familiar* and on which the cognitive mechanisms specific to *daily practice*[16] are triggered without difficulty. We will find that, in this phase, everyone suggests, under the impact of *"intuitive thinking"*,

[11] P. Iluț, *op. cit*.
[12] D. Kahneman, *Gândire rapidă, gândire lentă*, Editura Publica, București, 2012.
[13] P. Iluț, *op. cit*.
[14] *Ibid*.
[15] D. Kahneman, *op. cit.*
[16] P. Iluț, *op. cit*.

not much examined critically, an understanding of the socio-human reality. However, intuitive thinking has "*both amazing performances and deficiencies*"[17]. One of the major shortcomings of intuitive thinking is that it uses simplifying cognitive mechanisms that lead to a series of biases and heuristics that, although useful in everyday life, lead to misinterpretations (systematic errors) in the field of social and psycho-behavioural analyses. One of the main causes of the weakness of intuitive thinking is statistics. People, in general, according to D. Kahneman's analysis, are weak "*intuitive statisticians*". Of course, we also owe intuitive thinking the amazing performances in our daily life, with valid reactions or intuitions in everyday life. People, regardless of their status, are experts on many of the components of life and the decisions they make on these levels cannot be called into question. But from the point of view of the analysis of the starting socio-human situation/reality, the first level of analysis is not enough. We enter the second phase, one of deepening, investigation, understanding and scientific explanation, specific to the work of the social analyst. On this level, we try to release the biased content, to remove the systematic errors and the distorting effects, to apply valid and viable research tools, **to enter the epistemological laboratory for understanding the socio-human reality, striving to place research in the light of the axiological neutralism**.

A BRIEF HISTORY OF THE CONCEPT OF *"STRATEGY"*

In the usual vocabulary, in the most diverse fields, from economics to politics, from art to sports, from religion to science etc., there is no term used more than *strategy*. Moreover, for any individual, the setting of objectives and the planning of structured measures to achieve them may mean, depending on their own interpretation, that they have established either an action plan or a strategy. "*One person's strategy is another's tactic. What is strategic depends on where you are. It also depends on your timing: what seems like a tactic today, tomorrow might prove to be a strategy*"[18]. The terminological confusion between strategy and tactics, between strategy and project, between strategy and course of action etc., is due not so much to the semantic ignorance of concepts or to their excessive use for different situations, but to the fact that the pursuit of individual, group or organisational objectives represents, for some, a simple procedure, and for others, a real strategy[19]. Like any of the great concepts of the European cultural space, even if it comes from the military universe, the *strategy* one has its origins

[17] D. Kahneman, *op. cit.*
[18] James Brien Quinn, Henry Mintberg and Robert M. James, in "*The Strategy Process – Concepts, Contexts, and Cases*".
[19] *Ibid*, "*Human nature always tends to identify a definition for each concept. But maybe we fool ourselves by claiming that, for example, a concept such as strategy can be reduced to a single definition*".

in Greek antiquity. The term "*strategos*", prior to Pericles's period (450 B.C.), meant "*the art of a general*" describing the psychological and behavioural skills of one who occupies such a position[20]. The times evolved, but until the middle of the 20th century, the concept of strategy remained in the military terminological space, being implemented by doctrine, at the beginning of the 19th century, by Carl von Clausewitz, in the fundamental work of military strategy "*On War*". With the publishing of the paper "*Corporate Strategy: An Analytical Approach to Business Policy for Growth and Expansion*", in 1965, written by H.I. Ansoff[21], the concept of strategy is taken from the military area, semantically enriched and fully exploited in the economic field. Numerous documentary materials have then drafted that define, redefine and use the term *strategy* so frequent that from the second half of the 20th century until nowadays it has been used in any field, equally by specialists and by laypeople. Of interest is that the import of the term *strategy* into the economic scientific literature was made not only through a terminological takeover but also by importing its military doctrinal content. The criteria of analysis of an economic strategy are similar (on some levels, identical, such as concentration, flexibility, coordination, surprise, security, etc.) with those of a war strategy. In defining the *strategy* concept from the present research, one of the statements in the paper "*The Strategy Process – Concepts, Contexts, and Cases*", written by James Brien Quinn, Henry Mintzberg, and Robert M. James, will be used: "*a strategy is a pattern or a plan that integrates the goals, policies and action sequences (programs) of an organization into a fully functional whole ... The goals (or objectives) outline what needs to be achieved and when it will be achieved, but do not show how it will be achieved ... The big goals – those that affect the direction and viability of the entity as a whole – are called strategic objectives ... Policies are sets of rules or guidelines that show the limits between which actions must be maintained... Major policies – those that guide the direction and stance of the whole entities or determine their viability - they are called strategic policies ... The programs specify step-by-step the action sequences required to achieve the major objectives of the entity. They express how the objectives will be achieved within the limits imposed by the policies of the organization... These major programs that determine the general purpose*

[20] James Brien Quinn, Henry Mintberg and Robert M. James, in the above-mentioned book, remind us that in the beginning "*strategos*" meant a function (a general, at the command of an army). Then it was redefined as the *"art of a general"* that describes the psychological and behavioral skills of one who occupies such a position. During Pericles's time (450 BC), the concept is defined as the ability to command (in administration, through oratory, in positions of power). In the time of Alexander the Great (330 BC), it meant the ability to recruit forces to occupy a position and create a unified system of global governance.

[21] James Brien Quinn, Henry Mintberg and Robert M. James mention the book "*Corporate Strategy: An Analytical Approach to Business Policy for Growth and Expansion*" as one of the first scientific publications that addresses the use of the concept of business strategy.

and viability of the entity are called strategic programs". In this line of thought, a military strategic communication approach, part of a broader strategy, is nothing more than one of the fundamental programmes that aim to prepare the actual implementation of the strategy in an operational environment willing or even eager for a major military conflict to unfold.

IRRATIONAL AND RATIONAL, ASPECTS OF SOCIAL ACTION

If we operate the defining of the last generations of Australia born after 1965 in the terms stated by Mark McCrindle[22], and extrapolating the respective categories of populations born around the milestone between the millennia to the *"X", "Y", "Z"* cohorts from the other developed and emerging areas of the world, we find that, in the age of information and communication technology, we are both spectators and actors (populations X, Y, and Z) of a play in which we are living *live* the world paradox of the *manifestations of the individual and collective irrationality* against the background of the social reality built from technical decors, the material effects of rational thinking[23] developed progressively throughout the history of mankind to this date. If we also add to these cohorts the one born after 2010, the "*Alpha generation*", the beneficiary of the augmentation of the immediate reality or even of its replacement with *"virtual realities"* and which will probably be offered the undesirable opportunity to live in a period of global geostrategic rebalancing, including in the context of major military conflict, we can anticipate that the manifestations of individual and collective irrationality will not only continue

[22] According to Mark McCrindle, in the article "*Generations Defined*", an excerpt from *"The ABC of XYZ"*, broadcast through www.mccrindle.com.au, people born between 1965 and 1979 belong to the *"X"* generation; they lived their youthful years in relative peace and prosperity, before the crisis of September 11, 2001; people born between 1980 and 1994 are part of the *"Y"* generation (Millenials); they are living the crisis period after September 11, 2001; people born between 1995 and 2009 are part of the *"Z"* generation; they are living in a period of terrorism, global recession and climate change. According to the researcher, at present, four more generations are living alongside the generations presented above. These can all be understood (their attitudes, values, priorities and goals) if they are in agreement with the moment when they were born.

[23] Here, "*rational thinking*" is understood as a technical-scientific cognitive process that, throughout history, has brought humanity to the current technical and technological level. However, the "*rational"* of the current work to which the "*irrational*" will subsequently be referred to and defined – as an objective of understanding and a working tool in explaining "*irrational behaviour, whether individual, but especially collective*", falls within the paradigm of the "*critical rationalism*" of K. R. Popper, in which free people are constituted in an open society characterised by pluralism and tolerance and in which they solve their problems through dialogue, reason, condemning intolerance and totalitarian ideologies and, last but not least, the "*irrational*". Moreover, between the "*individual irrational*" – the one that generally manifests as a behaviour outside the predictability of the stage, by an action marked by the arbitrary and which is an effect of the genius of the social actor (of their intuition/vision) in anticipating the next stage, either the recurring effect of the individual's belonging to a social micro-network in a state of "*collective irrational*" – and the "*collective irrational*" itself, there is a difference of approach, since the "*collective irrational*" can be more easily identified and explained, including through the paradigm of approaching the human behaviour from an economic point of view, used in this paper.

on a planetary scale (possibly in transmissions through the most unusual communication channels), but they will also amplify. The extrapolation of the characteristics of the population categories of Australia to the developed and even emerging areas of the world was made on the basis of the similarities of psychosocial behaviour of the two spaces, in the context of globalisation (economic, social and even cultural), built mainly on the basis of technological and communication interconnection. Moreover, some of the irrational manifestations have as their starting point cognitive-cultural reactions that appear and extend, including throughout developed societies, as a result of the antagonistic ideological patents in niches (micro-networks) of the respective societies (social networks regarded as communication structures[24]), fully using the technological interconnectedness.

One of the fundamental concepts that will be launched in the debate is the (individual and collective) *"irrational"*, whose theoretical construction will be based on its antithesis to the *"rational"* of the Weberian type. The great German sociologist and economist, in his book *"The Protestant Ethic and the Spirit of Capitalism"*, speaks of the *"non-rational"*, which he defines by contrasting it with the *"rational"*: "*In fact, things are like this: one thing is non-rational not in itself, but from a certain "rational" point of view. For the non-religious man, any religious way of life, for the hedonist, any ascetic way of life is "non-rational" even though, measured by their ultimate value, they are a "rationalisation". If this study has any purpose, then it is to reveal the multilaterality of the concept – that appeared univocally – of the rational.*

The paradigmatic framing of the *"rational"*, in the context of communication relations, has many options. The structuralist-functionalist theories[25] provide the toolkit of factual characteristics through which one can decrypt the *"global network society"* and, above all, the criteria for delimiting the social micro-networks from its composition. Going one step further, the paradigm of the pluralism of social conflicts[26] explains, by identifying the centres of *"authority"* in the micro-networks, the balance that is established in the conflictual relations between different centres – authorities. On the other hand, through the game theory, the understanding of the ceaseless relationships of conflict, regulating the relations and establishing the balance state between the micro-networks focuses on the "*interdependence of the opponents' decisions and their expectations regarding the behaviour of the other*"[27].

[24] Manuel Castells, in the paper "*Communication Power*", defines "***the global network society***" as a **specific configuration of global, national and local networks in a multidimensional space of social interaction**. Not all people on the planet are included in this society, whose social structure is built around networks activated by micro-electronic devices, in which information that is processed digitally is transferred through communication technologies.

[25] L.A. Coser, *Les fonctions du conflict social,* P.U.F., Paris, 1982.

[26] R. Dahrendorf, *op. cit*.

[27] T.C. Shelling, *The Strategy of Conflict,* Cambridge, Massachusetts, 1980.

The economic approach to human behaviour[28], however, brings a more pragmatic note to an area of scientific interest that is, in fact, as far removed from the mirage of the abstract as possible, and which comes with applied answers to the need to propose efficient strategic communication plans in the age of the information technology and communication. Against this theoretical framework, the understanding of the "*rationality*" of social relations sits comfortably, while the economic "*irrational*" is out of the technicality of this theory. (For example: is a suiciding terrorist "*rational*" from the economic perspective of Gary S. Becker? What part of the suicidal terrorist's "*rationality*" is "*perverted rationality*"? What about a non-suicidal terrorist, can he have a "*rational*" argument for his deeds? Is his response a "*perverted rationality*" or is his behaviour simply a form of the "*irrational*"? So is the "*perverted rationality*" a form of the "*irrational*"?)

Max Weber suggests, in an attempt to remove the researcher from the biases[29] of the common sense, that "*the modern man in general, however willing he may be, is usually unable to imagine the importance of religious content of conscience for the way he lives, for the culture and character of the peoples; it is natural that we do not intend to put in place of a unilaterally "materialistic" causal interpretation of culture and history an equally unilateral spiritual one. Both are equally possible, but both serve as little to the historical truth if they were not intended to be a preparatory work but would claim to be an end of research".*

"THE GLOBAL NETWORK SOCIETY", A SUPERSTRUCTURE CONSTITUTED BY THE "SOCIAL MICRO-NETWORKS"

Within a network, the essential descriptive is "*the process by which it is reached – the communication that creates the connections between people and groups of people*"[30], i.e., the operating system of social networks, or of the social micro-networks if we look at them in relation to "*the society within the global network*". Moreover, one of the semantic content correspondences that we want to apply to "*social micro-networks*" is that of *audiences* because, in fact, we intend to reach them, as transmitters of messages from a military strategic communication campaign.

At the supra-state level, but not outside the state borders, we encounter a new form of society, identified by Manuel Castells as "*the global network society*"[31]. We are witnessing rapid and unpredictable techno-social transformations

[28] G.S. Becker, *Comportamentul uman – o abordare economică,* Editura All, București, 1994.

[29] D. Kahneman, *op. cit*.

[30] John Naisbitt, in "*Megatrends*", approaches the concept of networks frontally, defining them simply as "*people talking to each other, sharing ideas, information and solutions*".

[31] *Ibid.*

of societies[32] – existing within the nation-states – into global societies (increasingly) independent of their origin nation-states, of a process of globalisation even faster than the one intuited by M. Castells at the time he defined his new concept. In the context provided by the interference produced in the last years in the technological assembly of the communication information of *social media* type, on the one hand, and the cyber development and its interference with the most intimate spaces of the individual, on the other hand, we observe that in the "*global network society*", the "*social micro-networks*", the "*social media*" type of communities, extracted from the category of actual human communities, but different from their area of origin, are permanently, adaptively and algorithmically configured and reconfigured.

In the process of reorganising the "*global network society*" approach, there are also the political actors to be found, either those from the state nations or those which aim, in their effort to gain the power[33], larger, super-state spaces. In this sense, one of the fundamental criteria of political power, namely its territorial character[34], becomes somewhat diffuse in terms of obtaining and exercising power. The national state territory, in itself, remains, until a possible geostrategic rebalancing, defined by its political-administrative borders, but the areas of influence of the political actors exceed or are smaller than the territory and, implicitly, the sovereignty of the national state is affected, depending on the influences of other political actors, external ones, positioned in the social networks with a greater degree of influence[35] from the "*global network society*".

The key to the new social organisation of the communication type in which the structuring is achieved through the co-existence of the micro-networks that are

[32] Manuel Castells, in the paper "*Communication Power*", shows that *"the central technology of our time – communication technology – refers to the specificity of the human species: consciousness and meaningful communication".*

[33] The power defined by Max Weber in "*Wirtschaft und Gesellschaft" "means any chance used to impose your own will within a social relationship, even against resistance and regardless of the elements on which this chance is based".* The slightly conflicting note of the definition of power in the Weberian statement frames paradigmatically the use by the politician of coercive means "*against resistance*", which in a simple game of imagination can be military means, including their involvement "*against* external *resistance*" of the state represented by the political power in question.

[34] Jean Baechler, in the paper "*Le pouvoir pur*", argues that *"in order to be political, a power must begin by exercising itself in a confined space".*

[35] Manuel Castells, in "*Communication Power*", describes *"power"* as the relational capacity that allows a social actor to asymmetrically influence the decisions of another social actor/other social actors in ways that favour the will, interests and values of the strong actor. In the researcher's definition, the concept of "*actor*" refers to a variety of subjects of the action: individual actors, collective actors, organisations, institutions and networks. On the other hand, *"power"* is not an attribute, but a relation, more precisely, a relational capacity, with the considerations resulting from this statement, if the company is analysed from the perspective of the whole social networks from which it is constituted. The asymmetry in the definition of the concept of power tells us that, although the relation of influence is always reciprocal between the actors, in the case of the relation of power, one has a greater influence on the other.

inter-connected and in interference is globalisation. From this perspective, certain nodal centres of the networks become "*centres of power*", broadcasting a greater amount of meaningful content in communication, affecting decisively the degree of influence of the social actors. These, in an effort to adapt to the "*global network society*" level, develop relevant communication capabilities in the targeted social micro-networks, on the following levels of analysis:

1. an understanding of the mechanisms of constituting the "global network society" and, implicitly, the sociometric outlining of the "micro-networks" co-existing in the social influence area (the *"territory"*). The *"global network society"* is organised into distinct micro-networks, with several nodal (sometimes antagonistic) centres of power. Understanding involves the process of decryption of codes (communication protocols) and hierarchical mechanisms for transmitting objectives/messages between the constituent elements within the micro-networks. The extent of the process of communication between several elements leads to the establishment of the existence of that social micro-network itself, and the level of the process of communication of elements within the micro-network leads to the establishment of the power hierarchy of these elements within the micro-network. The social micro-networks are different in terms of the planimetry of their constituent elements and have dynamic structures (of the nodal distribution in the geographical territory), but they are similar in function in their binary system (of the inclusion or exclusion of the constituent elements in one or the other of the micro-networks). A social micro-network with more stable geography and evolution in the dynamics of the more predictable structure is one in which the transmission of influence through the nodal centres is made easier.

2. identification of power relationships within micro-networks. Social systems are, by definition, conflicting, being generated continuously as a result of the balances resulting from the relocation race of power relations over time. The *"global network society"* not only remains one of the conflicts between the social actors/social micro-networks but, given its structure, it is one in which the conflictual state is accentuated, the balance having a higher degree of lability. Some nodes become centres of power, setting (programming), on the one hand, the objectives (meaning and content of social micro-networks) and, on the other hand, the ideologies (the operating procedures of the micro-networks in order to achieve their goals).

3. evaluating the distance between the nodal centres of the social micro-networks and establishing the degree of interference between the micro-networks, either in the common nodal centres of retransmission or in the common ones of power. The degree of interference, within the whole *"global network society"*, modulates the transmission of the influences of the social actors. Under conditions of competition between the actors, the transmission

becomes asymmetrical, depending on the relational capacity and, above all, on their potential to penetrate simultaneously and adaptively more micro-networks. In the interference points, if the distance between the network nodes located in at least two micro-networks tends to zero, the respective interference points become centres of simultaneous transmission of the influence of the social actors in several micro-networks. The absence of interference zones between the nodal centres or the random interference of the constituent elements of the networks, which are not important in terms of power relations within these micro-networks, lead to an increase in the influence distance between the micro-networks and, consequently, to an increase in effort to transmit the influence of the interested social actors. An infinitely increased distance between the nodes of some micro-networks leads to the break of the inter-nodal communication links.

The increase of the degree of the lability of the nodal centres, around which the social micro-networks are constituted, induces, therefore, an increased accentuation of the conflicting nature of the social micro-networks. Understanding the *"global network society"* as a superstructure consisting of distinct and dynamic structures – *"social micro-networks"* – leads to the conclusion that the degree of organic stability of today's society has diminished as a result of the different organisational stability of social micro-networks and of their status rebalancing. On the other hand, the opening up towards a conflicting state of the *"global network society"* further alleviates the instability generated by the micro-networks in the conflicting relationship. The formulation is thus maintained from a structural-functionalist perspective, in the 1967 set of statements by the American sociologist Lewis A. Coser[36].

AN APPEAL TO THEORY

The *"game theory"* is one of the current approaches applied to the field of confrontation of two major political actors, among which a "*paradoxical strategic balance*" [37] is achieved. Thomas Shelling, the author of this idea, believes that "*even in the most destructive strategic confrontations there can be created, paradoxically, by the simple logic of confrontation and mutual threat, points of balance and elements of cooperation and consensus between the two sides*". The conclusions of the American sociologist on the line of maintaining the strategic balance, but also his references on the "*rational*" versus the "*irrational*", from the new strategic thinking of the great planetary players confirm the degree of interest for the subject

[36] L.A. Coser, following some analyses on small groups, issued a series of scientific statements, results of empirical research.

[37] T.C. Shelling, *op. cit.*

and guide the analysis of these concepts in the context of their transposition in order to understand the way of relationship structure of the *"global network society"*.

In the literature, strategic communication receives multiple and nuanced conceptual framings, depending on the organisational sphere to which it is confined. Strategic communication is an activity deliberately adopted by an organisation in order to embed in the collective mind of its audience an image that will allow it to achieve its major organizational objectives.

In a simplified perspective, strategic communication can be defined as being a creative process carried out by an organisation within a set period of time, through which the organisation's "*messages*", "*transmission channels*" and "*audiences*" are interconnected in order to achieve the status end of the organisation. We observe that, over time, the three elements have undergone refining stages, due in large part to the development stages of human society. Thus, the "*messages*" received subtle content, the "*transmission*" began to take place in real-time, and the "*audiences*" were fragmented and often over-specialised. Moreover, in the relationship between the three elements, in the current social context, the "*audiences*" borrowed functional characteristics of "*messages*" and "*transmission channels*". If the "*messages*" are properly constructed and delivered, the "*audiences*" themselves become a multiplier and transmitter towards themselves and externally.

It was, therefore, natural from the planners of strategic communication to increase the attention in their analysis of multiple "*audiences*". To a rigorously and/or psycho-socially defined "*audience*", it may be appropriate to deliver tailored messages (algorithmically) so that the major objectives of the communicators are achieved.

Narrowing the area of defining strategic communication in order to channel the research towards its own area of interest, we note that, on a military level, NATO, through its strategic communication agency, defines this process as "*integrating the communication capabilities and information functions with other military activities in order to understand and model the information environment. By information environment we mean not only the information itself but the individuals, organizations and systems that receive, process and transmit the information and the cognitive, virtual and physical space in which they take place*"[38]. StratCom, NATO's strategic communications agency, is currently carrying out major communication campaigns, so that its political-military objectives are realised, according to the interests of the organization[39].

[38] https://www.stratcomcoe.org/

[39] Starting with December 2017, a strategic NATO communication campaign called #WeAreNATO is being run in Romania, which aims precisely at the high school and university population's understanding of the role of NATO for the member states, in general, and for Romania, in particular.

Starting from the previous theoretical considerations, we open the analysis towards the topic of major political actors[40] and the possibility for them to intensify a given political situation to an extreme, reaching a major military conflict, the interstate war, in the context of the *"global network society"*. Intra-state conflicts are also the result of extreme conflictual political situations, the way of establishing the balance between the intra-state political actors, for example through a civil war (social actors with a bigger or lesser relevance in their struggle for power within an internal social system) not being the object of this analysis. Therefore, the political actors, in their attempt to obtain and maintain power, transpose the political situation of balance between the states into a state of war between these. According to Carl von Clausewitz's statement[41] of two centuries ago, "*war is only a continuation of politics by other means*." Even though the doctrinal approaches to conducting a war are much changed from the moment the author made one of the most systematic theorisations of the major military conflict in human history, the sociological intuition regarding placing the war in the area of political struggle for power has been confirmed today, the great orders of operations, on the basis of which the armed forces are engaged, are nothing more than the transposition into normative-military framework of the intention of the major political actor, a deciding factor for using the military as a political instrument. The military strategies themselves are drafted after the commander has acquired the political intention of the great social actors and its transformation into military strategic objectives. However, war is one of the social processes with evolutions difficult to predict, its evolution depending on numerous variables, some of them, at the beginning of the war, remaining perfectly unknown.

In this context, the commander's intuition in formulating strategic objectives differentiates between a course of action of the subordinate forces (even at a strategic level, which may or may not be successful) and a military strategy. Through the military strategy, the commander engages not only the belligerent force in the major conflict but also introduces (*irrationally*), among the strategic elements, vision elements for the military organisation, that go beyond common sense.

[40] Because the analytical approach follows the communication process of a state military institution at the preamble stage of a major military conflict, such as the war between at least two state entities, the political actors are defined as major, these being represented by the central governmental structures of a state, responsible for the initiation or participation imposed in the respective war.

[41] Carl von Clausewitz, in "*On War*", considers that "*war is not just a political act, but a real political instrument, a continuation of political relations, an accomplishment of them by other means"*. In such a conflictual relationship, the political intention is the purpose, the war being nothing more than the means of achieving the intention.

Among the elements necessary for waging war[42], together with their commander (and their armed forces) and government, Carl von Clausewitz introduces the "*people*" in which, before the actual start of the war, "*the passions meant to ignite a war*" should pre-exist (the collective irrational). This is a topic that all major political actors are concerned about, who, before communicating their extreme decision, i.e. to use their armed forces, as the last resort of the political intention, build the support of the society they represent by inducing the ideas of justice and legitimacy of the action of the belligerent state. Thus, in the pre-war phase, military strategies are formulated, but as a first (essential) step, in order to ensure the support of the people, a set of campaigns/strategic communication plans are implemented.

CONCLUSIONS

The epoch schema of the structural change of the society occurred when the information technologies started interfering in the mechanisms of social structuring. It started two decades ago, it has become acute and grown exponentially in recent years. The transformation of the structure of the social classes (outside the individuals) did not keep pace with the rhythm of the technological interference within the structure as a whole, so that the initial social equilibrium state based on social hierarchy and axiological connections turned into a state with multiple equilibria of autarchic micro-networks (by the decision of individuals), less stable, based on proximity of values and collective irrationality.

The mechanisms of decision-making in the state political field are fuelled, on the one hand, by the ideological and axiological reflections of national and extra-national societies, with an identifiable degree of logical coherence and, on the other hand, to an increasing extent, by the reactions to the stimuli of the collective irrational, logically inconsistent, random and latent.

In the field of electoral strategies, the political representatives have gone from the stage of identifying and persuading large categories of voters (major categories of the social structure), based on general sociological characteristics, to the stage of understanding the gregariousness characteristics of social micro-networks - distinct audiences, adapting and detailing their political messages so that they respond to elements of collective irrationality that arrange the respective substructures.

The major military conflict, especially if there is the possibility of its occurrence in the proximity area of a state, re-hierarchizes the psycho-social anxieties – including

[42] In the above-mentioned book, Clausewitz considers war "*a strange trinity, composed of the original violence of its element, hatred and enmity, which must be regarded as a natural blind instinct, of the game of probabilities and of chance, which make war a free activity of the soul, and from the subordinate nature of a political instrument, through which it returns to the pure intellect*".

for the generations of a population that have not directly experienced the socio-economic consequences of a war -, bringing into manifestation the mechanisms of collective thinking that existed latently in the collective mind, including especially from the typology of the collective irrational.

Strategic decisions of state authorities are practically reflected in the state military system by drawing up action and response/contingency plans, including by developing and implementing strategic communication plans.

Strategic military communication represents the integration of communication and information capabilities with other military activities aimed at modelling the information environment according to the objectives of the military institution[43]. Strategic communication comes into operation in the earlier phases of a military operation, being a precursor to the stages of the military action itself.

In the early phases of its manifestation as a social phenomenon, the hybrid type war has the aspect of using an unconventional arsenal in which information and communication technology becomes a weapon through which certain elements of the society are targeted that produce social and/or economic disorder and social micro-networks through which states of social anguish are induced (distrust in the elements of national authority). In this phase, the operational environment is viewed as extended in comparison with a possible area of armed conflict and the targets mainly target segments of the civilian environment.

The military system imports and adapts the functioning mechanisms of the strategic communication carried out by the great electoral and / or economic actors in order to initiate and apply either offensively or counter-offensively the strategic communication campaigns assumed as vectors of persuading the populations from the operational environments, according to the political decisions of the state authorities.

Strategic communication, given the age of information technology and generalized communication, remains, on the one hand, an instrument within the reach of any organization, regardless of its relative size, if transmission channels and messages with viral distribution and replication (viralisation) qualities are used in the social micro-networks constituted in the cyber-space of the social media and, on the other, a waste of resources regardless of the economic power of an organisation, if it is planned and organized without a careful understanding of the different audiences, of the prior identification of the social micro-networks to which it is addressed.

[43] https://www.stratcomcoe.org/

BIBLIOGRAPHY

1. R. Ackermann, C. Eden, *Strategic Management of Stakeholders: Theory and Practice*, Elsevier, 2011.
2. G.S. Becker, *Comportamentul uman – o abordare economică*, Editura All, București, 1994.
3. C. Bockstette, *Jihadist Terrorist Use of Strategic Communication Management Techniques*, George C. Marshall Center for European Security Studies, 2008.
4. R. Boudon, *Tratat de sociologie*, Editura Humanitas, București, 2006.
5. Bryman, *Social Research Methods*, OUP Oxford, 2012.
6. M. Castells, *Communication Power,* OUP Oxford, 2013.
7. D. Chiribucă, *Metode de cercetare a comunicării și mass-media,* Editura Didactică și Pedagogică, București, 2014.
8. D. Chiribucă, *Communication: Theories, Frameworks and Processes,* Editura Eikon, Cluj-Napoca, 2013.
9. Carl von Clausewitz, *Despre război*, Editura Militară, București, 1982.
10. L.A. Coser, *Les fonctions du conflict social*, P.U.F., Paris, 1982.
11. R. Dahrendorf, *Class and Class Conflict in Industrial Society*, University Press, Stanford, 1967.
12. R.M. Grant, *Contemporary Strategy Analysis*, John Wiley & Sons Ltd., West Sussex, United Kingdom, 2010.
13. P. Iluț, *Problematizări și explicitări ale cunoașterii socioumanului*, in "*Psihopedagogie specială. Modele de evaluare și intervenție*", Editura Polirom, 2015.
14. P. Ispirescu, *Basmele românilor*, Editura Polirom, 2012.
15. D. Kahneman, *Gândire rapidă, gândire lentă*, Editura Publica, București, 2012.
16. J. Naisbitt, *Megatendințe. Zece noi tendințe care ne transformă viața*, Editura Politică, București, 1989.
17. M.M. Neag, *A New Typology of War – The Hybrid War*, "*Nicolae Bălcescu*" Land Forces Academy, Sibiu, 2012.
18. J.B. Quinn, H. Mintzberg, R.M. James, *The Strategy Process – Concepts, Contexts, and Cases*, Prentice Hall, Englewood Cliffs, New Jersey, 1988.
19. R. Rughiniș, R. Deaconescu, G.G. Milescu, M. Bardac, *Introducere în sisteme de operare*, Editura Printech, București, 2009.
20. T.C. Shelling, *The Strategy of Conflict*, Cambridge, Massachusetts, 1980.
21. Cdr S.A. Tatham MPhil RN, *Strategic Communication: A Primer*, UK Defence Academy, 2008.
22. I. Ungureanu, *Paradigme ale cunoașterii societății*, Editura Humanitas, București, 1990.
23. M. Weber, *Etica protestantă și spiritul capitalismului*, Editura Humanitas, București, 1996.

THE USE OF KEY PERFORMANCE INDICATORS (KPI) AS USEFUL DECISION-MAKING AND PERFORMANCE IMPROVEMENT TOOLS IN THE ACCEPTANCE OF THE *BALANCED SCORECARD* CONCEPT

Gheorghe MARCU
PhD Candidate, "Carol I" National Defence University, Bucharest

Radu Mihai OANȚĂ
PhD Candidate, "Carol I" National Defence University, Bucharest

Toma PLEŞANU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Cătălin BURSUC, PhD
Professor, "Carol I" National Defence University, Bucharest

The Balanced Scorecard (BSC) concept is defined and used in managerial practice as a measurement system, as well as a strategic planning and management system, being implemented in business or industrial organisations, in the government system, or non-profit organisations.

From the efficiency of management point of view, Balanced Scorecard uses Key Performance Indicators (KPIs) to measure performance within the organisation, through which it can add direct corrections in design, initiatives and daily activities for the achievement of strategic organising objectives.

This article presents the role of Key Performance Indicators regarding the evaluation of the actions taken, the decision-making and the overall efficiency of the organization's activity. Due to the concepts and functions developed within the Balanced Scorecard (BSC), rigorous determination of performance and counter-performance within an organisation (KPI), Balanced Scorecard (BSC) and its instrument of evaluation are also recommended for use in institutions within the defence, public order and national security system.

Keywords: Balanced Scorecard, Key Performance Indicators (KPI), organisation, national defence.

INTRODUCTION

The complexity and especially the dynamics that can be observed in the evolution of contemporary society on all its economic, political, diplomatic, social, scientific and military levels require proactive conduct on the part of decision-makers, regardless of their field or level. This behaviour must be based on a forecast, identification of possible evolutions of the reference system, analysis of existing risks and vulnerabilities, prioritisation of available resources, development of appropriate answers to all predicted situations or to those situations with unpredictable developments.

Any organisation, regardless of the nature and object of its activity, cannot be run without taking into account the functions of management[1]: forecasting, organising, commanding, coordinating, and controlling. This whole process is under the direct command and responsibility of the management team, which plays the main role in defining the strategy, the strategic objectives, developing policies and implementation plans, controlling actions, in other words, in the general orientation of the entire range of activities specific to the organisation in the long term.

Modern management is based on a scientific approach due to the various trends and principles stated and confirmed over time, the introduction of the command and control act automation within the organisations, the existence and development of the IT tools and technologies that provide the support of the management activities. This impact can be observed throughout the whole range of specific managerial activities (planning, organisation, management, training, communication), with a higher impact on the analysis and evaluation of the own actions taken (control).

In the military organisation also, one can easily observe the existence and employment of all management functions, in each of the specific military fields, as well as in all military daily activities and actions: *the forecasting function* – the field of military information; *the organisational function* – personnel and mobilisation, training; *the command and control function* – essential in the employment of military instruments and principles; *the evaluation function* – required to obtain the feedback on the assigned/undertaken actions.

The functions of management are characterised by interdependence and a certain succession over time. They are characterised by dynamism and directly

[1] Henry Fayol, *General and Industrial Management*, published by Martino Fine Books, 2013, reprint of the 1949 edition.

linked to scientific-technical progress. The functions of management have their characteristics but also universality in the whole range of actions in which they are taken:

- the forecasting and planning function includes analysing the existing and future risks and own vulnerabilities, establishing the strategy, objectives, policies, programmes, procedures, initiatives, time and budget;
- the organisational function determines the organisational structure, establishing the chain of command and control, delegating and empowering, defining the missions and tasks within the organisation;
- the management and coordination function is responsible for assigning tasks and levelling out efforts, training the military, coordinating the budget execution, setting priorities for reaching the goals, motivating the personnel, establishing the space-time coordination, and the internal and external communication;
- the evaluation function is focused on setting performance standards, evaluating and interpreting the results in terms of efficiency, ensuring the processes correction measures.

Strategic objectives are undoubtedly the central element of management. Addressed as quantitative or qualitative expressions, subsumed to the purpose of the establishment and raison d'être of the organisation, they represent the reference points in transforming the organisation, fulfilling the strategy and bringing the vision to fruition. They generate responsibility at all levels: individual, group or organisation ones.

Characterised by the acronym SMART[2] (Specific, Measurable, Achievable, Relevant and Time-bound), the strategic objectives are also subject to the control and evaluation function. This process determines the factual status of the organisation, compares the measured and recorded results with the planned level of ambition, analyses the positive or negative evolution and makes the necessary corrections to align the effort with the strategic objectives.

Performance management applied at the organisational or individual level reflects the progress made and the results achieved in the implementation of the strategy and strategic objectives.

At the military-strategic level, the performance evaluation can be interpreted as the key to the successful implementation of the organisational transformation and the procurement of modern military equipment. At the military operational level, we can talk about the success achieved in aligning the entire institutional effort in implementing the strategy and achieving the strategic objectives.

[2] George T. Doran, *There's a S.M.A.R.T. Way to Write Management's Goal and Objectives*, in *Management Review*, pp. 35-36, November 1981.

The military tactical level corresponds to the evaluation of the performance at individual and microstructure level, the performance of the tasks within the assigned terms, the quality of the works, performance in training and education etc.

BALANCED SCORECARD CONCEPT

The Balanced Scorecard (BSC) concept, introduced by Robert S. Kaplan and David P. Norton, in 1992, is focused on improving performance. It includes a series of measures regarding the evaluation of organisational, financial and non-financial performance, in a single score sheet and evaluation. Over time, it has received several improvements, now being considered a concept with multiple features:

- management and control systems;
- performance management system;
- strategic communication system.

The innovation of the BSC concept consists of introducing new concepts in the evaluation of the performance of an organisation, in addition to the classical ones and mainly the financial ones, such as: employee competencies/skills, employee motivation, innovation and employee continuous training, as well as the recorded and evaluated values classification in four large quadrants/perspectives:

- The financial perspective;
- The customer perspective;
- The internal processes perspective;
- The learning and growth perspective.

BSC assists the command team in the early identification of the problems that have the potential to transform into obstacles to the implementation of the strategy.

Due to the high level of flexibility, the applicability of the BSC concept in the military system is proven by the success of the foreign armed forces that adopted and implemented it[3]: Royal Navy, US Air Supply, Babcock International Group etc.

The conclusions derived from analysing the application of the BSC concept in the defence sector are the following[4]:

- the BSC should not be viewed strictly from the performance evaluation function, but must be approached as a tool for directing the evolution and transformation of the military organisation;
- the BSC enables the strategy to be clarified and communicated throughout the organisation, aligning the individual and institutional effort in achieving the strategic objectives;

[3] http://www.ebalncedscorecard.ro, retrieved on 03.08.2019.

[4] Gheorghe Marcu, *Analiza conceptului Balanced Scorecard și aplicabilitatea acestuia în organizația militară*, in *Univers strategic*, January-March 2019, year X, no. 1(37), Editura Creștină *"Dimitrie Cantemir"*, București.

- to ensure the successful implementation of the BSC, the direct involvement and support by the command team is required.

The implementation of the BSC concept in the military organisation leads to the improvement of the overall performance of the military field, the successful implementation of the reforms, the transparency of the activities and decision-making processes, the continuous adaptation of the military body to the internal and international realities, to the achievement of the strategic objectives.

The specialised literature highlights the essential characteristics specific to the control-evaluation process:

- relevance – the process must be tailored to the specific activity of the military organisation and its personnel;
- flexibility – the dynamics of external factors also manifests itself within the military organisation; for this, it is necessary to continuously adapt the control-evaluation process in order to meet the realities in the field;
- focus on critical issues – analysis and evaluation should be directed to the results of those processes with major impact in carrying out actions that contribute to objectives achievement;
- simplicity, clarity – the evaluation must be easy to perform, and the results must be easy to analyse; the time factor is most often decisive in adopting a corrective or prophylactic response;
- cost-efficiency – the control and evaluation process is a cost generator; they must not exceed the activity under analysis.

KEY PERFORMANCE INDICATORS

The control and evaluation function is very important for the evaluation of the organisational performance, although it is given less attention in the managerial processes.

Performance management is a process by which the progress made in meeting the objectives is evaluated, including here the efficiency of using the available resources (human, financial and information ones) for achieving the assigned measures, the quality of the results and the evaluation of the way the individual and collective effort is tailored to meet the strategic objectives. Performance management starts with determining what we want to evaluate, identifying methods of collecting data and information, collecting, analysing and evaluating them, interpreting and making corrective decisions, whenever necessary. The control-evaluation process must be continuous to become effective, with increased intensity on the key points, at key moments, and on the staff in charge of the duties.

Among the benefits of the performance management process, there are three important aspects that must be highlighted:

- it provides the necessary feedback in the decision-making process at all levels – strategic, operational or tactical one;

- it assures excellence in the processes, initiatives, plans that contribute to the accomplishment of missions and tasks;
- it ensures the implementation of the corrective measures on the processes, initiatives, or plans even from the initial manifestation phases that reflect a deviation from the planned natural course; identifying centrifugal sources and trends and correcting them supports continuous and consistent improvement.

The BSC concept places at the disposal of the command team a set of tools that make up the image of the military organisation, up to date and without distortions: the critical success factors and the key performance indicators. By implementing this set of factors, further by analysing and interpreting them, a system of levers is created through which the organisation continuously improves its performance.

Critical Success Factors (CSF) and Key Performance Indicators (KPIs) are two very common terms met in the literature. The difference between the two terms is represented by the difference between cause and effect.

Within the strategic management, the determination of the strategic objectives represents a process by which the management team sends the long-term directions of action to the organisation. The BSC concept teaches us that these have to be evenly distributed across the four quadrants, they do not have to be numerous, their role being to guide the daily activity of the staff.

A CSF is, in fact, a high-level performance objective, associated with a strategic objective that must be achieved by the organisation. Critical success factors are the cause of success, they determine what needs to be done to achieve success.

The CSF is constituted as a benchmark pre-set by the management team that becomes an objective of the joint efforts of the personnel, required to be reached or even exceeded. Once these benchmarks/thresholds are established, achieving them ensures alignment of the organisation with the defined strategic objectives.

We must emphasise that our approach to determining the performance within the military organisation starts from the hypothesis of the existence of the state of peace, in all other military states (pre-conflict, deterrence, conflict, post-conflict, armed struggle) it is based on other principles, methods, and tools through to ensure success in facing the opponent.

To be effective, a critical success factor must[5]:

- *"be vital for the successful implementation of the organisation's strategy;*
- *bring benefits to the department responsible for its implementation, as well as the entire organisation;*
- *be synonymous with a high-level objective;*
- *be directly connected with the strategy of the military organisation".*

[5] https://www.clearpointstrategy.com/how-to-determine-critical-success-factors-for-your-business/, retrieved on 12.06.2019.

To identify the critical success factors, a comprehensive and interdepartmental internal analysis is needed to identify the key elements of the strategic objectives that support the vision and mission of the military organisation. While the strategy sets the mission and objectives of the military organisation (i.e. what we aim/want to achieve), the CSFs show us how we will achieve it, the minimum accepted thresholds that we must reach.

The specialised literature offers a series of analysis methods that lead to the correct identification of critical success factors:

- OAS (Objective, Advantage, Scope) statement and analysis;
- SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis;
- analysis of the strategy implementation plan;
- structural change/modification of the military organisation.

As a method for the choice of the critical success factors, a set of questions can be used to highlight their weight in the process of implementing the strategy[6]:

- Does the choice of this factor lead to the desired result?
- Are the conditions ensured to achieve the desired result?
- What resources are needed to achieve this objective?
- Do the personnel of the organisation possess the skills necessary to achieve this objective?

The identification and selection of critical success factors must also take into account their equal distribution in the four perspectives, the success of the implementation of the strategy being based equally on the success in the whole range of actions of the military organisation.

In this way, the CSF provides the necessary context for the personnel of the military organisation to route their daily effort towards the essential activities and on the priority regarding the tasks that must be accomplished, setting the minimum threshold necessary for the accomplishment of the tasks.

On the other hand, KPI represents a punctual measure in the evaluation of an objective, a value that refers to the threshold defined by the CSF and that by comparison gives us indications regarding the degree of achievement of the measured objective.

The key performance indicators are the basic tools in the evaluation, obtaining important data and information concerning the definition and achievement of the objectives.

KPIs are tools that by their application return data and information of a qualitative or quantitative nature, variable in time and space and which by their further interpretation describe the degree of achievement of the set objectives.

KPI is a measure of performance, specific to an organisation, in a particular area.

[6] https://bernardmarr.com/default.asp?contentID=1406, retrieved on 12.09.2019.

The units of measurement used in the description could vary from fundamental one-dimensional units (hours, meters, kg, litre etc.) to multidimensional units of measurement (personal ratio in/out of the system, consumption recorded per kilometre/nautical mile, number of training exercises per year etc.), the measurement offering complex and qualitative information related to the different parameters that need to be evaluated.

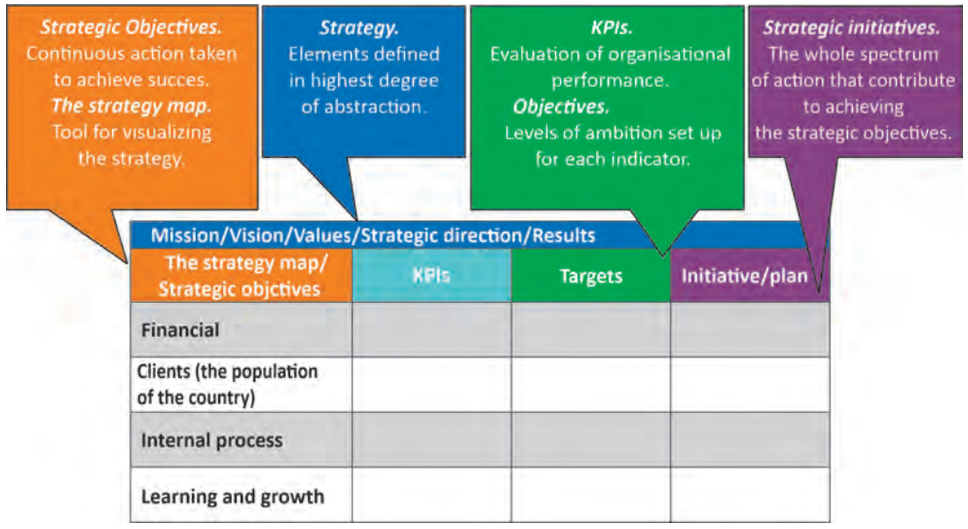


Figure 1: The role of performance indicators in the Balanced Scorecard concept

Source: adapted from https://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard, retrieved on 26.08.2019.

The best Key Performance Indicators are those that are linked to strategic goals and priorities. The popularity of tables and graphs gives an overview of the entire spectrum of activities in progress, at one point – the score table.

The literature offers thousands of KPIs and, if we set out to measure everything, it would be a completely meaningless, costly and time-consuming exercise. It should not be overlooked that the registration of the values for the KPIs established to be monitored at the command level will be carried out to by the personnel of the unit, increasing the responsibilities in the job description and reducing the time required to carry out the current activities. Therefore, key performance indicators should be thought of as a way to easily quantify the organisation's goals and priorities in quantifiable measurements. Using these values, in tabular or graphic format, the command team will be able to evaluate the performance of the military organisation, at the level of the individual, microstructure, department or the organisation as a whole.

The key performance indicators, when evaluating the activities of a department in relation to the operational and strategic objectives, can return values that reflect: the recorded result, which can then be evaluated in comparison with the planned one; the evolution trends of the activities included in the plans; the general effect generated in the organisational set: internal and external strategic communication.

Also, the key performance indicators can still return values that can detect:

- where the military organisation is at any given time;
- performance evolution, comparatively, at predetermined time intervals;
- reaching previously defined thresholds (maximum or minimum) to ensure rapid corrective responses;
- diagnosis of the military system for identifying the problems of process, human, technical, organisational, budgetary, time-bound;
- predictability in the strategy implementation process.

In choosing those parameters to be measured, quantified and recorded, a balance must be established between the quantity (total number of KPIs, the frequency of recording and reporting, the level of detail established to be quantified, the reporting chain etc.) and the quality of the results obtained. In the quantitative evaluation of the key performance indicators, both the accepted minimum thresholds and an accepted range/margin can be introduced in which the measured values can be located.

In addition to the key performance indicators, another set of indicators must be analysed and introduced in the equation of efficiency and effectiveness of actions carried out by the military organisation: risk indicators. Defined in a broader sense, the concept of risk refers to the extent of the mismatch between different possible outcomes, more or less favourable or unfavourable, in a future action. It expresses the possibility of recording deviations from the planned purpose[7].

Within the actions carried out in the military organisation, the daily analysis of the situations provides data and information based on which the command team and the General Staff identify, analyse and accept risks or plan actions to avoid/diminish their impact.

The risks encompass the entire spectrum of activities and all areas specific to the military organisation. Within the organisational framework, risk designates a complex phenomenon resulting from the relationship between the probability of success and the failure of an action aimed at the goal, with significance at the individual or collective level[8].

[7] Ion Coteanu, Luiza Seche, Mircea Seche (coord.), *Dicționarul explicativ al limbii române*, Editura Univers Enciclopedic, București, 1998, p. 929.

[8] Dumitru-Cătălin Bursuc, *Modele, metode și instrumente pentru identificarea și evaluarea factorilor majori de risc în organizațiile militare*, (doctoral thesis), București, 2015, p. 31.

The key risk indicators constitute a warning system for the command team in case the direction of action of the military organisation departs from the ordered direction.

While performance indicators answer the question *What should we do to achieve the strategic objectives?*, the key risk indicators answer the question *What can prevent us in achieving the strategic objectives?*

The key risk indicators can be defined independently, measured and recorded separately or associated with the key performance indicators by setting minimum or maximum thresholds/intervals in their metric evolution, manifesting outside the established margin, constituting a risk in achieving the strategic objectives.

All measured values, at predefined time intervals, will be entered into a database. By interrogating it and using defined interfaces, we can illustrate the current situation on the ground and the evolution trends of the initiatives in real-time. The interpretation of the results and the application of the corrective measures on the actions of the subordinates depend on the preparation of the command team, the experience gained, as well as the intuition of the commander in the perspective evaluation of the phenomenon.

In conclusion, the algorithm proposed by the Balanced Scorecard concept for evaluating the management implementation of the strategy starts with the clear definition of the vision, the mission and the strategic objectives, the establishment of the implementation plans, the definition of the CSF factors that must be established in order to reach these objectives and the evolution of things with the support of the KPI, in order to observe if the military organisation carries out its entire spectrum of activities at an optimal level of performance.

The focus of the command team must also be on the choice of those initiatives, plans, processes, specific processes that enable the action of the individual and the whole organisation to achieve the strategic objectives.

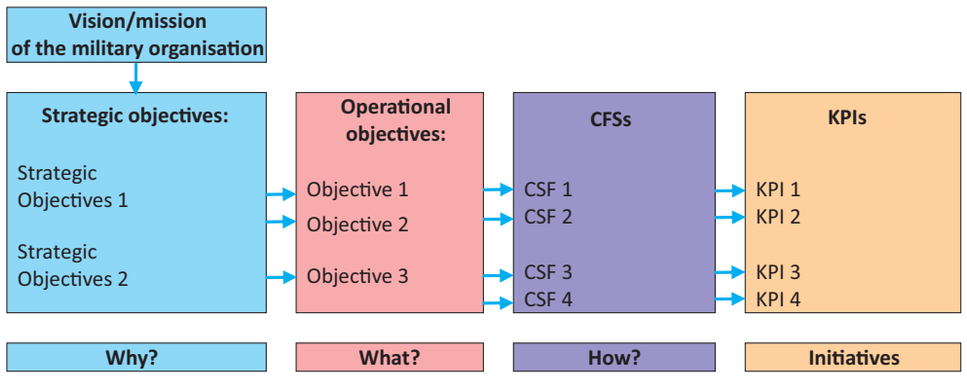


Figure 2: Matrix map regarding the interconnection of the strategy and the operational level

Source: adaptation to *Notes on Balanced Scorecard* by Glen Alleman (*Performance-Based Project Management: Increasing the Probability of Project Success*, American Management Association, 2014).

The analysis and capitalisation of the results obtained from the field by following the threshold reached in the implementation of the operational objectives will enable the command team to evaluate the alignment of the military organisation to the strategic objectives and, if necessary, to make the necessary corrections. The measures adopted start from minor corrections (reviewing implementation initiatives, assignments and including project managers, allocating resources etc.) and can reach the following range of deeper measures[9]:

1. Organisational restructuring. It involves reducing staff, number of departments or combining them, the number of hierarchical, pyramidal structures. The reduction of military personnel must be viewed from the perspective of international commitments, the degree of stability and regional, and international security;

2. Reengineering. The basic idea from which we start with this concept is the following: essential for the success of the implementation of the strategy is not primarily the availability of resources (financial, material, human, informational), but an optimal organisation of the activity, based on criteria of prioritising the wanted effect. It focuses on optimising internal processes, redefining and redistributing tasks and improving internal performance criteria. In other words, the personnel structure of the military organisation and its degree of readiness correspond to the requirements for the fulfilment of the strategic objectives, but an internal reorganisation is needed regarding the distribution of tasks and the allocation of financial and material resources to optimise the entire process and achieve the strategic objectives.

3. E-Engineering. This is the equivalent of the previous measure, in which the IT dimension is amplified in the entire spectrum of activities of the organisation. Expanding the computer network, increasing the level of network security, increasing the level of classified information conveyed in the network, acquiring specialised software to support the daily and specific activity of each department, training of IT personnel are all challenges that support such an approach.

Finally, we propose a relevant example that demonstrates the need to align all aspects that contribute to the success of implementing a strategy. The example we propose is developed for a military tactical-level logistics unit intended for current repairs within the Navy Forces.

Mission

The military unit will ensure the maintenance of the fighting technique on board the military ships.

[9] Fred R. David, *Strategic Management. Concepts and Cases*, Tenth Edition, Pearson Education International, Prentice Hall, 2005, pp. 255-257.

Strategic objectives

- Strategic objective 1: maximizing the operational level to ensure the full spectrum of current repairs onboard military vessels;
- Strategic objective 2: continuous improvement of personnel training.

Performance objectives

- performance objective 1: ensuring the hiring of qualified personnel and their continuous training;
- performance objective 2: endowment with state-of-the-art technical equipment;
- performance objective 3: ensuring the repair of defective equipment during the shortest time;
- performance objective 4: contracting of specialised courses from the manufacturers of military equipment.

Critical success factors

- CSF 1: active promotion in the local and national media of career opportunities in the naval field;
- CSF 2: the allocation of financial resources for the purchase of last-minute diagnostic equipment and equipment and for carrying out external specialisation courses;
- CSF 3: training of the staff in the use of existing and newly acquired equipment;
- CSF 4: training of staff so that each person is double specialised.

Key performance indicators

- KPI 1: staffing degree> 90%;
- KPI 2: technical assurance degree with repair equipment / diagnostic equipment> 90%;
- KPI 3: daily allocation of a 1-hour interval for on-the-job training using existing or newly purchased equipment;
- KPI 4: staff turnover by 10%, within the technical departments, at 6 months.

CONCLUSIONS

Human society is going through a new era, the informational one, characterised by easy access to information and a great capacity for trading information. The informational avalanche on the management team has a direct and not always positive impact on the decision-making process. More information increases the degree of uncertainty, which can be easily manipulated for purposes contrary to strategic objectives.

The dynamics of change in the external organisational environment require flexibility and adaptive and rapid responses. The impact assessment on the effects

generated by the decisions made is included in the same equation of the relatively short time available. Current conditions also focus on the workforce that has skills and knowledge above the average recorded in previous years, but also on the expectations it has from the environment in which they work.

The clear definition of a strategy, the vision regarding the organisational path, the description of the strategic objectives, the expectations from the staff facilitate the daily activity of the individual in the present information bombardment. The objectives, strategic or operational, act as institutional benchmarks in the decision-making process at the individual, microstructure or command team level. It also supports aligning the individual and institutional efforts to achieve the vision and implement the strategy.

One of the dimensions of the Balanced Scorecard concept that can be adopted and which can determine immediate effects within the military organisation is the use in the process of evaluating the institutional performance of critical success factors (CSF) and key performance indicators (KPI).

Obtaining the correct data from the right person at the right time allows the command team to make better informed, faster decisions, which are fully consistent with the reality on the ground.

The control and evaluation of the organisational path become a mandatory component in the managerial process. The use of Key Performance Indicators, with the support of computer applications, leads to a real and overall picture of the entire spectrum of activities carried out by the military organisation. The selection, measurement, analysis, and evaluation of the key indicators also ease the task of the command team in the decision-making process, focusing on the revealing and impact factors recorded during the implementation of the strategy.

By implementing performance management, it will be possible to keep the course of the military structure in the parameters of excellence in relation to its missions, national or derived from the ally status of Romania.

BIBLIOGRAPHY

1. Dumitru-Cătălin Bursuc, *Modele, metode şi instrumente pentru identificarea şi evaluarea factorilor majori de risc în organizaţiile militare*, (doctoral thesis), București, 2015, p. 31.
2. Fred R. David, *Strategic Management. Concepts and Cases*, Tenth Edition, Pearson Education International, Prentice Hall, 2005, pp. 255-257.
3. George T. Doran, *There's a S.M.A.R.T. Way to Write Management's Goal and Objectives*, in *Management Review*, pp. 35-36, November 1981.
4. Henry Fayol, *General and Industrial Management*, Published by Martino Fine Books, 2013, reprint of 1949 Edition.
5. Robert S. Kaplan, *Conceptual Foundations of Balanced Scorecard*, Working paper, Harvard Business School, 2010.

6. Robert S. Kaplan, David P. Norton, *Using the Balanced Scorecard as a Strategic Management System*, in *Harvard Business Review*, 1996.
7. Robert S. Kaplan, David P. Norton, *The Balanced Scorecard: Translating Strategy into Action*, Harvard College, 1996.
8. Robert S. Kaplan, David P. Norton, *The Balanced Scorecard – Measures That Drive Performance*, in *Harvard Business Review*, 1992.
9. Robert S. Kaplan, David P. Norton, *The Execution Premium: Linking Strategy to Operations*, Harvard Business School Publishing Corporation, 2008.
10. Costel Loloiu, Toma Pleșanu, Dumitru-Cătălin Bursuc, *The Resistance to Change as a Specific Risk for the Organization Transformation*, in *Journal of US-China Public Administration*, Volume 12, No. 8, August 2015, pp. 593-602.
11. Gheorghe Marcu, *Analiza conceptului Balanced Scorecard și aplicabilitatea acestuia în organizația militară*, in *Univers strategic* Review, Editura Creștină *"Dimitrie Cantemir"*, year X, nr. 1(37), București, January-March 2019.
12. Gheorghe Marcu, Dumitru-Cătălin Bursuc, Toma Pleşanu, *Analysis of Balanced Scorecard Efficiency for Implementation into the Field of National Defence*, Proceedings of the 10th International Conference on Knowledge Management: *Projects, Systems and Technologies*, November 2017, Editura Universității Naționale de Apărare *"Carol I"*, București, pp. 163-169.
13. Gheorghe Marcu, Dumitru-Cătălin Bursuc, Toma Pleşanu, *Short Analysis on the History and the Evolution of the Balanced Scorecard Concept*, Proceedings, The 14th International Scientific Conference Strategies XXI, April 2018, Editura Universității Naționale de Apărare *"Carol I"*, București, vol. I, pp. 327-333.
14. Gheorghe Marcu, Dumitru-Cătălin Bursuc, Toma Pleşanu, *The Logic Pyramid of Balanced Scorecard Strategic Planning*, Proceedings of the 14th International Scientific Conference Strategies XXI, April 2018, vol. I, Editura Universității Naționale de Apărare *"Carol I"*, București, pp. 333-341.
15. Paul R. Niven, *Balanced Scorecard Diagnostics: Maintaining Maximum Performance*, John & Sons, Hoboken, NJ, 2005.
16. Paul R. Niven, *Balanced Scorecard Step-by-step for Government and Nonprofit Agencies*, Second Edition, John Wiley & Sons, Inc., 2008.
17. Toma Pleșanu, Dumitru-Cătălin Bursuc, Costel Loloiu, *Dedicated Risk Management Software*, Proceedings of the 9th International Conference on Knowledge Management *"Knowledge Management: Projects, Systems and Technologies"*, 26-27 November 2015, Editura Universității Naționale de Apărare *"Carol I"*, București, pp. 125-129.

WEBOGRAPHY

1. http://www.ebalncedscorecard.ro, retrieved on 03.08.2019.
2. https://www.clearpointstrategy.com/how-to-determine-critical-success-factors-for-your-business/, retrieved on 05.09.2019.
3. https://smartkpis.kpiinstitute.org/kpi-101/characteristics-of-good-kpis, retrieved on 19.08.2019.
4. https://bernardmarr.com/default.asp?contentID=1406, retrieved on 12.09.2019.

STRATEGIC MAP – PLANNING INSTRUMENT FOR THE SUCCESSFUL IMPLEMENTATION OF THE TRANSFORMATION STRATEGY IN THE ACCEPTED MEANING OF THE *BALANCED SCORECARD* CONCEPT

Gheorghe MARCU
PhD Candidate, "Carol I" National Defence University, Bucharest

Radu Mihai OANȚĂ
PhD Candidate, "Carol I" National Defence University, Bucharest

Toma PLEŞANU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Sorin-Gheorghe PÎNZARIU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

The Balanced Scorecard (BSC) concept is defined and used in managerial practice as a measurement system, as well as a strategic planning and management system, being implemented in business or industrial organisations, in the government system, or in non-profit organisations.

In order to align the individual and collective efforts, respectively to create an effective internal communication channel, the Balanced Scorecard concept provides an instrument with a strong visual and motivational impact – the strategic map.

The strategic map creates the overall picture of the organisation, the objectives and the implementation way for strategy, enables the employees to be aware of their own effort that contributes to the success of the implementation of the strategy and realises the framework of their own and institutional self-evaluation regarding the effectiveness of the actions taken.

In this article, we will address the essential elements of a strategic map, the way of defining and selecting them, the relationship and interdependence of the elements and we will recommend a strategic map starting from the vision, mission and transformation strategy existing in the military structures of the operational level.

Keywords: Balanced Scorecard, strategic map, aligning efforts, organisation, national defence.

INTRODUCTION

The principles and methods which are used in management have been defined, refined and confirmed or denied in the organisational practice, by the contribution of numerous authors and researchers from various fields, of which we mention: Frederick Taylor, Henry Fayol, Peter Druker, Dale Carnegie, Michael E. Porter, Henry Mintzberg and many others.

The evolution of human society, in general, is based on two causes: an internal need, self-improvement, and an external one, dictated by the achievement of the efficiency and effectiveness of the actions taken, respectively the maximisation of the profit. Thus, permanently found in human attention and concerns, the science of organising and managing human activities is characterised by a continuous evolution of conceptual definitions, methods or instruments of interpretation, application, and evaluation, the final aim being to optimise the ways, means, and resources used to reach the set objectives.

Strategic management involves defining the vision and the mission, implementing the strategic objectives and initiatives, all of these formulated by the management team positioned at the top of the organisational hierarchy, starting from an evaluation of the internal and external environment in which the organisation operates and which is based on existing or potentially existing resources.

Introduced in 1992 by Robert S. Kaplan and David P. Norton, the *Balanced Scorecard (BSC) concept* is part of the social sciences field which provides tools, concepts, principles, and rules linked to strategic management. The authors of the BSC are pioneers in introducing in the evaluation of the organisational and strategic performance of the non-financial indicators, besides the financial ones, as well as the grouping of all of them into four quadrants[1]:

- financial perspective;
- customer perspective;
- internal processes;
- development and improvement.

Balanced Scorecard is a concept used in both private and public sector organisations, used to point out/highlight the vision, missions, strategic objectives of an organisation, to evaluate the performance of strategic management and to be

[1] Robert S. Kaplan, David P. Norton, *The Balanced Scorecard – Measures that Drive Performance*, Harvard Business Review, 1992.

used as an effective internal communication tool.

Transformation processes, which also include performance management, are difficult for each organisation, bringing unique challenges into discussion and analysis. However, by using the Balanced Scorecard, public sector organisations share best practices and become organisations that focus on strategy by[2]: mobilising executive management, translating strategy into terms of operation, sequencing and aligning strategy within their organisations, communicating everyone's strategy within the organisation, ensuring that the strategy is an ongoing process, evaluating the strategic performance and correlating the actions with the available resources.

The transformation of organisations and implicitly the initiation of reform elements that aim to increase the efficiency in meeting the objectives acquire a specific configuration when we talk about organisations in the national defence system. This properly understood and applied specificity can be a facilitating element that leads to a sustained change or, on the contrary, a delay element[3].

In the new age we are going through, the information age, which can be described as a complex and vast three-dimensional matrix of data and information, the cause-effect relationship manifests itself omnidirectionally, in the whole range of activities and domains. The decision-making process thus becomes more complex and difficult to manage, being necessary to establish/define benchmarks that enable the decision-maker, as well as the subordinate staff, to identify the optimal solutions within the established limits and the available resources. The ability and efficiency with which the tasks are carried out become vital for the survival of the organisation. At the same time, the multiplication and distribution of these benchmarks are a very effective internal communication tool for aligning the individual and organisational effort for the fulfilment of the strategic objectives.

To support the entire strategic transformation process, BSC provides the command team with a very practical internal and external communication tool – the strategic map, which allows the entire staff effort to be aligned to achieve the strategic objectives and the desired end state, respectively creating an external, transparent image of the institutional effort.

The implementation of a strategy implies directing the organisation from a present point and moment to a definite end state, but uncertain as a result, the development of the actions towards reaching the objectives being subject to the cause-effect relationship. The strategic map presents in a comprehensive, explicit

[2] Patricia Bush, *Strategic Performance Management in Government: Using the Balanced Scorecard*, Cost Management, Boston, Vol. 19, Issue 3, May/Jun 2005, pp. 24-31.

[3] Dumitru-Cătălin Bursuc, *Analysis of Resistance to Change as a Specific Risk of Military Organization*, International Scientific Conference *"Strategies XXI"*, vol. 2, suppl. Centre for Defence and Security Strategic Studies, Editura Universității Naționale de Apărare "Carol I", București, 2014, pp. 231-237.

and easy-to-follow form the whole chain of inter-conditions and inter-relationships between the performance objectives set within each quadrant and which competes in meeting the strategic objectives and achieving the vision.

The organisational management approach through the BSC directs the military structure towards flexibility, performance, efficiency, and progress in carrying out the assigned missions.

APPLICABILITY OF THE *BALANCED SCORECARD* CONCEPT IN THE MILITARY ORGANISATION

To apply the BSC concept in the military organisation, it is necessary to adapt the principles, concepts, and instruments to the specificity of the military field from the perspective of the four perspectives:

- *financial perspective*: optimisation of the operating costs of the military organisation and ensuring efficient management – cost savings and efficiencies;
- *customer perspective*: transparency in the spending of public money and the degree of confidence that the population gives to the military organization – customer satisfaction;
- *internal processes perspective*: adapting the organisational structure to formulate an optimised response to internal and external challenges; aligning the internal effort to support the vision and achieving the strategic objectives set; optimising the internal and strategic communication process – quality of military services;
- *learning and growth perspective*: ensuring the conditions for attracting young personnel and subsequently developing them within the institutional framework, according to the needs of the military organisation; ensuring an informative technical system to support the decision-making act – culture and leadership.

Financial perspective. From the military point of view, this perspective cannot be evaluated from the cost/revenue ratio. In general, for the government institutions, the value returned to the social system concerns concepts such as education, health, safety, and security of the citizen and cannot be generically quantified in financial terms as profit. In the field of defence, it can be evaluated through transparent decision-making policies regarding the allocation of budgetary funds, the operational substantiation of the needs of procuring with military equipment, the prioritisation of the projects according to the allocated funds, the efficient spending of the allocated funds.

Customer perspective. From this perspective, as far as the military organisation is concerned, we are witnessing a conceptual restriction, its offer being addressed first of all to the population, to the Romanian nation and closely followed by the commitments and obligations that the Romanian military has within the various alliances. It can be evaluated by the degree of confidence entrusted by the population in the armed forces in carrying out the constitutional missions.

Internal processes perspective. This perspective sets the objectives by which the military organisation maintains a high degree of training to successfully carry out the ordered missions, optimises its internal operating processes, establishes the internal framework for the promotion of military values, promotes transparent and efficient management in the spending of public money.

The challenge we identify in this process is the identification of those internal processes and their cyclic evaluation (out of the multitude that can be set to meet the objectives), processes that compete decisively in meeting the strategic objectives.

Learning and growth perspective. This perspective can be considered as the basis and engine of all other perspectives. To achieve all the proposed objectives, a personnel policy is needed to maintain and develop the skills of the employees at the level of the existing technical requirements and specific to the field of each one.

It includes three directions of action: human capital, organisational structure, and information technology. All the activities carried out to achieve the objectives are based on the human resource, its degree of training, the ability of the military organisation to model its organisational structure according to the constitutional missions and, last but not least, the use of the latest information technology that ensures the efficiency of the whole spectrum of military activities and technical support in making, disseminating, evaluating and implementing decisions – automating the management act.

Organisational transformation processes can be influenced by several positive or negative factors. One of the factors with a strong impact is the legal, normative framework. The support of the process of adaptation and implementation of a new strategy must be based on a legislative framework that endorses the strategic decisions at the conceptual level, but also at the one of the allocation of resources. The allocation of insufficient funds can lead to delays in the implementation of the plans and initiatives, the manifestation of the domino effect in the internal processes and the learning and growth, finally leading to the impossibility of carrying out the tasks and missions assumed.

The pressure of time can have an effect on getting solid results and ensuring continuity in the implementation of the strategy. It is essential to look realistically at the time and resources needed to achieve the goals. Most organisations that successfully implement a performance management process speak of medium

periods of five to seven years before the actual results are obvious. However, this can be problematic for many organisations in the public sector, respectively the military field, because the changes occurred in the command teams every four years need and require continuity in the adopted plans of implementation without making any personal corrections. The coherence and consistency of the actions of the command teams create the optimal environment for achieving the performances and aligning the institutional effort with the achievement of the strategic objectives and the accomplishment of the missions.

To successfully implement the Balanced Scorecard concept in the military organisation, it is necessary to take into account the experiences, observations, and lessons learned within the other public, military or private organisations in their effort to implement the concept, reduce or even eliminate those negative factors that may influence the process of organisational transformation.

Today, Balanced Scorecard is presented as a concept with multiple features:

- strategic management and control system;
- performance management system;
- strategic communication tool.

The aforementioned features are just as many advantages that recommend the BSC concept for use in the situation of restructuring and reorganisation of macro components of the military organisation and of improving the institutional performance.

STRATEGIC MAP

The strategic map integrates the whole BSC concept for the implementation of a new strategy and the improvement of organisational performance. The successful implementation of the BSC is based on the accurate illustration of the cause-effect relationships between the strategic objectives of the organisation established within the four quadrants. A strategic map is a tool that makes connections between the strategic objectives and the processes that contribute to the implementation of the strategy. It provides the command team and the staff with a simple and transparent vision, through which they can coordinate and evaluate their daily activities.

The strategic map is the main internal and permanent communication tool that can be used by the command team in the relationship with subordinates. For the transparency of the military administrative act, the strategic map can also be used as an external communication tool, to inform citizens about the processes and priorities of the military organisation. It presents in a brief form and with a strong visual impact the main directions in which the effort of the whole group must be routed, allowing the staff to use it in the daily activity as a criterion for prioritising their activities or received tasks.

The performance objectives or key objectives included in the four quadrants reflect the need for action and effort direction, and they are expressed through an affirmation of what needs to be done in order to align with the strategy. In order to meet the condition of efficiency, it is necessary that the objective is formulated in an instrumental way, being important that its definition starts with the active verb.

Active verbs are used for this purpose: to create, initiate, maintain, develop, excel, build, improve, activate, reduce, assist, accelerate, increase, support, encourage, identify, modify, produce, facilitate, navigate, achieve, assures, allocate, translate, invent, coordinate, maximise, minimise etc.

For the effective coordination of the whole strategy, it is recommended that the vision, the desired end state or the mission of the military unit should be written at the top of the strategic map.

The process of defining and choosing the objectives in the four perspectives becomes the most important step in the Balanced Scorecard concept. Based on the key objectives and the established plan for their evaluation, the degree of performance set is achieved in the management of the implementation of the strategy and the organizational transformation.

From a ***financial perspective***, the key objectives that can be included in a strategic map can be:

- allocation of budgetary resources to ensure the training and equipping of the army at the level of the modern demands of the battlefield;
- implementation of efficient management that ensures transparency in the spending of public money and optimisation of the operating costs of the military organisation.

The ultimate goal of the financial perspective is to ensure a multiannual and continuous financial exercise that allows the transformation of the armed forces into modern armed forces capable of responding to current or future challenges.

In the process of identifying the performance objectives from the ***client perspective***, they must start from the expectations or requirements that the armed forces must meet in order to ensure success in the assigned missions. Here we can list:

- organisational and structural alignment with NATO and EU best practices;
- providing state-of-the-art military and technical equipment;
- issuing legislative projects that lead to the attraction of military and civilian personnel (the attractiveness of the military system), respectively the loyalty of the existing one;
- participation in international military actions under the auspices of the UN, NATO or EU in order to train a professional military body (the capabilities and skills of the Romanian military personnel, acquired during participating

in NATO missions, are the basis for increasing the level of professionalism necessary for the planning and deployment of military actions in a multinational framework, under different geopolitical, relief and climate conditions, customs and cultures etc.).

The ultimate goal of this perspective is to continually adapt own possibilities to counteract the present and future threats.

From the ***perspective of internal processes***, the performance objectives for ensuring the performance of strategic management must be pursued:

- adaptation of the command and control structure corresponding to the force structure;
- initiation of major procurement programmes for modern military equipment and equipment;
- revitalisation of existing military equipment and equipment systems;
- joining the force categories in the research and development projects of new military capabilities, within the national or NATO/EU framework;
- automation of the command and control process from tactical to strategic level;
- development of fighting and protection capabilities in cyberspace;
- moving up cooperation and training jointly with NATO, EU or international partners, regionally or all over the world;
- development of internal and external communication as a way of raising awareness of the role of each man within the military system within the collective effort of the organisation to transform itself into modern armed forces;
- continuous assessment of the risks due to the unpredictable evolution of the regional or international security environment, to ensure a maximum and decisive military response.

This perspective aims to continuously adapt the organisational structure and procurement to formulate an optimised response to the challenges of the international environment.

The ***learning and growth perspective*** introduces in the process of evaluating the performance of an organisation concepts such as: competencies/abilities of the employees, internal motivation of the employees, innovation etc., notions that were not evaluated in the past, the evaluation organisational performance being predominantly based on financial values[4].

[4] Toma Pleşanu, Cătălin-Dumitru Bursuc, Gheorghe Marcu, *Analysis of Balanced Scorecard Efficiency for Implementation into the Field of National Defense*, Proceedings of the 10th International Conference on Knowledge Management *"Knowledge Management: Projects, Systems and Technologies"*, 23-24 November 2017, Editura Universității Naționale de Apărare *"Carol I"*, București, 2015, pp. 163-169.

The following performance objectives can be assigned to the personal and innovation perspective:

- reorganising the military education system to ensure the formation of graduates according to the new requirements imposed by the technical, technological and IT development;
- developing the individual or collective training component through the virtual simulation of the battlefield;
- establishing legislative measures to ensure the conditions for attracting young staff and subsequently its institutional development tailored to the needs of the military organisation;
- providing an informational technical system to support the decision-making act;
- implementing human resource management that will contribute to the creation of a performance climate by establishing the recognition of the efforts made, innovating and rewarding these actions;
- aligning the individual or collective effort in achieving the performance objectives and improving the performance of the military institution.

Once completed, the strategic map presents the following advantages[5]:

- it provides in a visual, simple, clear and easily accessible format a graphic representation of the main operational objectives; this way of mapping the strategy is visually appealing; it is much easier to remember a map of the strategy than something written in an agenda or disseminated through an e-mail; moreover, it can be added on the institution's website and displayed inside the institution, on the halls or inside the rooms;
- it helps to identify key strategic objectives that really and decisively contribute to the achievement of strategic goals, mission accomplishment, and vision;
- it allows a better understanding of the elements described in the strategy and on which it is necessary to intervene to improve the process;
- it unifies and aligns all operational objectives with the mission and vision defined by the command team; it translates the operational language specific to each department in a language easily understood by all military and civilian personnel;
- it provides each employee with a clear objective to be retained and to be applied in the activity of performing the tasks and tasks; failure to disseminate the strategy to command staff and subordinate units will maintain a state of confusion regarding the alignment of the institutional effort;

[5] Robert S. Kaplan, David P. Norton, *Strategy Maps: Converting Intangible Assets into Tangible Outcomes*, Harvard Business School Publisihing Corporation, 2004, pp. 29-56.

- it helps to realise the image of inter-conditioning and inter-relation of the strategic objectives arranged in the four perspectives; the failure or the success reached in the achievement of an objective propagates in the chain throughout the mechanism of support and implementation of the strategy; we can say that the entire organisation functions as a strategic ecosystem: small changes can have a decisive impact on the functioning of the whole, leading to malfunctions and even blocking the organisation in functioning and achieving the proposed objectives.

The strategic map presents, conceptually, some failures. According to some authors, the main shortcoming of the strategic map is the lack of time dimension for the temporal delimitation of the objectives and processes that it contains. However, from the perspective of implementing a new strategy, organisational transformation within a military organisation, with terms placed between medium to long term, from 10 to 15 years, the time dimension loses relevance, the focus is on identifying and implementing those solutions that support the whole process throughout its duration.

Also, when drawing up the strategic map for the military organisation, it starts from two basic perspectives:

- the internal perspective, through which we have the BSC concept for identifying those objectives, processes, policies, initiatives or plans for the realisation and implementation of the strategy, of their interconnection and inter conditioning;
- the external perspective – the regional and international security environment that also affects and could shape the entire organisational transformation process.

From these two perspectives, great attention must be paid to the continuity in time of the objectives transposed in the strategic map. The identification and choice of the strategic objectives included in the strategic map is the result of a process of analysis of the existing internal situation, specific to the organisation and analysis of external factors and with major impact on the country and implicitly the military organisation (type analyses: PESTLE – political, economic, social, cultural, technological, ecological, legal; MOST – mission, objectives, strategy, tactics; SWOT – strengths, weaknesses, opportunities, vulnerabilities).

In the medium and long term, the assumptions from which the strategy was developed and implemented change, the initial predictability being replaced with the internal evolution recorded through the implementation of the transformation policies/plans and with the external evolution of the security environment. The unpredictable evolution of the external security environment can lead to the modification of the defence strategy with direct effects in the transformation and adaptation of the military body to the new threats.

This dynamic should not be seen as a need to restore the entire process of strategic analysis and transformation, but only as a need for continuous evaluation and redefinition of strategic objectives and priorities in the evolution of the military body. An alternative solution may be the existence of several strategic maps designed based on the scenarios elaborated at a strategic level regarding the evolution of the international security environment.

Starting with the definition of the strategic objectives, followed by the drawing up of the strategic map, the identification of the performance and risk indicators, we can move on to the next stage: defining the strategy implementation plan, practically the staging of the initiatives/activities during the entire strategic cycle.

Finally, we propose a relevant example in which we present a Strategic Map in which we have included: the main operational objectives for Navy, defined in the context of existing realities.

CONCLUSIONS

We conclude the brief review of the role and importance of the strategic map in achieving the motivational support regarding the implementation of the transformation strategy by presenting the principles set out by Bob Paladino in a paper he wrote in 2011 regarding the framework needed to ensure that the organisation achieves superior performances:

- establishment of a normative framework and a responsive structure that allows the continuous evaluation of the activities;
- continuous improvement and internal communication of the strategy: the strategic map coupled with the Balanced Scorecard allows the employees to easily visualise how they can support the organisation's goals;
- configuration of the strategy by sampling, disseminating and establishing responsibilities within the organisation: monitoring, through the Balanced Scorecard and the pre-determined key performance indicators, the manner and degree of meeting the operational objectives;
- continuous improvement of performance: the strategic map and the Balanced Scorecard highlight the points where the organisation must coordinate its resources and efforts to reach the strategic objectives;
- knowledge management and capitalisation: once the problems identified are solved, the exchange of best practices and knowledge disseminates the solutions adopted within the organisation for the efficiency of internal processes.

The strategy map ensures the transformation of the strategy into operational objectives, delimited in the four perspectives, but interconnected and interdependent in a cause-effect chain.

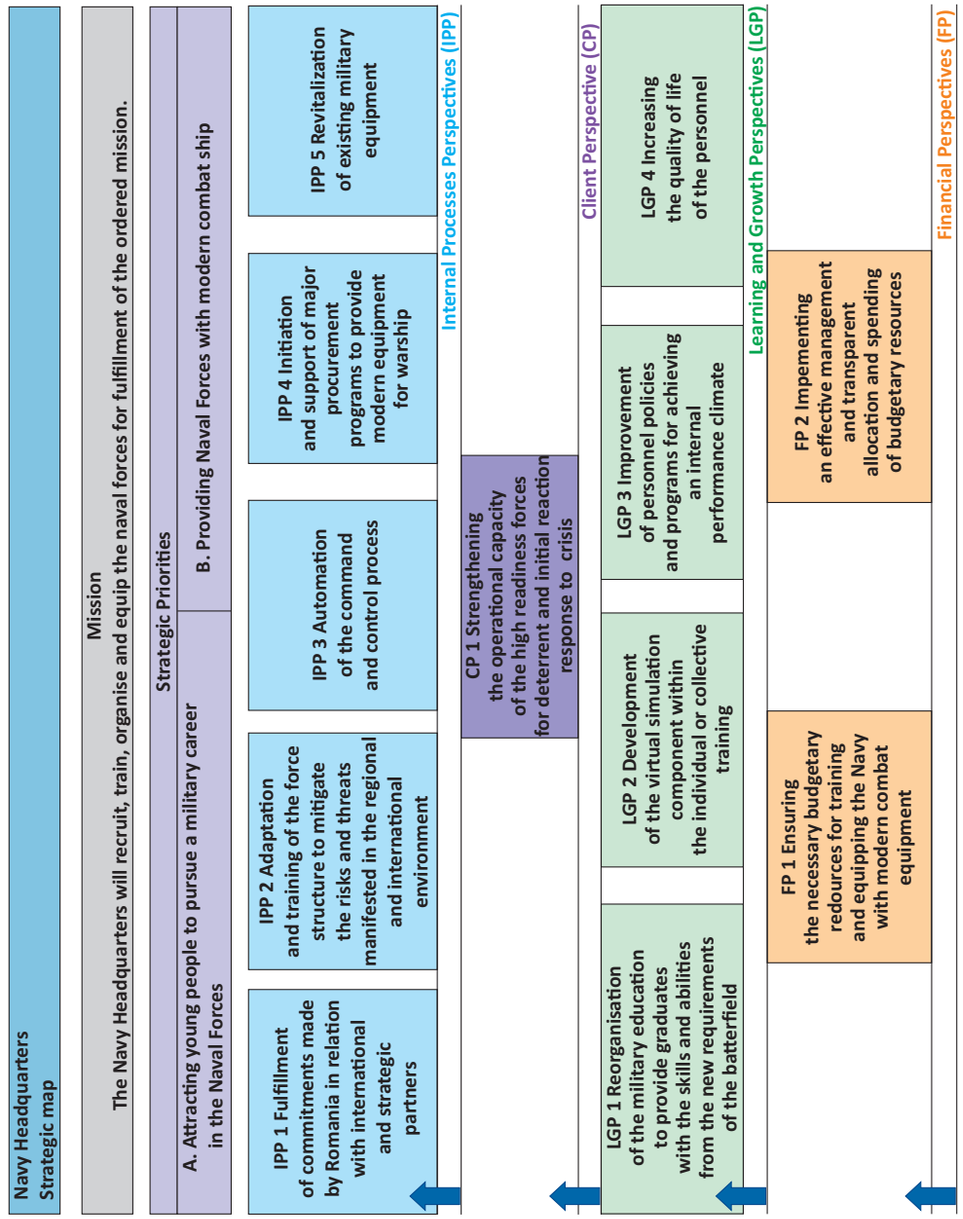


Figure no. 1: Strategic map for the Navy (model)

Organisations that wish to succeed in implementing the strategy need effective communication in their daily activity so that each person/organisational structure fulfils the tasks and responsibilities. The efficiency and effectiveness of internal communication within the organisation are the basis for motivating and providing useful information to the members of the organisation.

The strategy map is the instrument by which the operational objectives of the military organisation are defined and assumed by the command team, causally related, interdependent and interconnected, while also representing a communication channel of the strategy within the military organisation, to the lower echelons, subordinates as well to the central structures. It is the foundation of creating an organisational culture focused on achieving strategic objectives and materialising the vision.

This dissemination within the military organisation plays a decisive role in aligning the efforts of all military and civilian personnel in carrying out daily tasks and achieving operational objectives.

Balanced Scorecard is today the basis of a performance management system that uses strategic, operational and individual level plans for the implementation of fundamental processes of communication, monitoring, and improvement of the organisation's performance[6].

BIBLIOGRAPHY

1. Dumitru-Cătălin Bursuc, *Modele, metode şi instrumente pentru identificarea şi evaluarea factorilor majori de risc în organizaţiile militare*, (doctoral thesis), București, 2015, p. 31.
2. Patricia Bush, *Strategic Performance Management in Government: Using the Balanced Scorecard*, Cost Management; Boston, Vol. 19, Issue 3, May/Jun 2005, pp. 24-31.
3. Robert S. Kaplan, *Conceptual Foundations of Balanced Scorecard*, Working paper, Harvard Business School, 2010.
4. Robert S. Kaplan, David P. Norton, *Strategy Maps: Converting Intangible Assets into Tangible Outcomes*, Harvard Business School Publishing Corporation, 2004.
5. Robert S. Kaplan, David P. Norton, *The Balanced Scorecard – Measures That Drive Performance*, in *Harvard Business Review*, 1992.
6. Robert S. Kaplan, David P. Norton, *The Balanced Scorecard: Translating Strategy into Action*, Harvard College, 1996.
7. Robert S. Kaplan, David P. Norton, *The Execution Premium: Linking Strategy to Operations*, Harvard Business School Publishing Corporation, 2008.

[6] http://www.ebalancedscorecard.ro/pages/conceptul-bsc, retrieved on 12.09.2019.

8. Robert S. Kaplan, David P. Norton, *Using the Balanced Scorecard as a Strategic Management System*, in *Harvard Business Review*, 1996.
9. Robert S. Kaplan, David P. Norton, Bjarne Rugelsjoen, *Managing Alliances with the Balanced Scorecard*, Harvard Business Review, January-February 2010.
10. Costel Loloiu, Toma Pleșanu, Dumitru-Cătălin Bursuc, *The Resistance to Change as a Specific Risk for the Organization Transformation*, in *Journal of US-China Public Administration*, Volume 12, No. 8, August 2015, pp. 593-602.
11. Edwin A. Locke, *Motivation by Goal Setting*, Harvard Business Review, November 2001.
12. Gheorghe Marcu, *Analiza conceptului Balanced Scorecard și aplicabilitatea acestuia în organizația militară*, in *Univers strategic* Review, Editura Creștină "Dimitrie Cantemir", year X, nr. 1(37), București, January-March 2019.
13. Gheorghe Marcu, Dumitru-Cătălin Bursuc, Toma Pleşanu, *Analysis of Balanced Scorecard Efficiency for Implementation into the Field of National Defence*, Proceedings of the 10th International Conference on Knowledge Management: *Projects, Systems and Technologies*, November 2017, Editura Universității Naționale de Apărare *"Carol I"*, București, pp. 163-169.
14. Gheorghe Marcu, Dumitru-Cătălin Bursuc, Toma Pleşanu, *Short Analysis on the History and the Evolution of the Balanced Scorecard Concept*, Proceedings, The 14th International Scientific Conference Strategies XXI, April 2018, Editura Universității Naționale de Apărare *"Carol I"*, București, vol. I, pp. 327-333.
15. Gheorghe Marcu, Dumitru-Cătălin Bursuc, Toma Pleşanu, *The Logic Pyramid of Balanced Scorecard Strategic Planning*, Proceedings of the 14th International Scientific Conference Strategies XXI, April 2018, vol. I, Editura Universității Naționale de Apărare *"Carol I"*, București, pp. 333-341.
16. Paul R. Niven, *Balanced Scorecard Diagnostics: Maintaining Maximum Performance*, John & Sons, Hoboken, NJ, 2005.
17. Paul R. Niven, *Balanced Scorecard Step-by-step for Government and Nonprofit Agencies*, Second Edition, John Wiley & Sons, Inc., 2008.
18. David P. Norton, Randall H. Russell, *Best Practices in Managing the Execution of Strategy*, Balanced Scorecard Report, July-August 2004.
19. Bob Paladino, *Five Key Principles: Corporate Performance Management*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.
20. Toma Pleșanu, Dumitru-Cătălin Bursuc, Costel Loloiu, *Dedicated Risk Management Software*, Proceedings of the 9th International Conference on Knowledge Management *"Knowledge Management: Projects, Systems and Technologies"*, 26-27 November 2015, Editura Universității Naționale de Apărare *"Carol I"*, București, pp. 125-129.
21. http://www.ebalancedscorecard.ro/pages/conceptul-bsc, retrieved on 12.09.2019.

THE USE OF QFD IN BUILDING UP A KNOWLEDGE BANK IN THE FIELD OF DEFENSE, PUBLIC ORDER AND NATIONAL SECURITY

Radu Mihai OANȚĂ
PhD Candidate, "Carol I" National Defence University, Bucharest

Gheorghe MARCU
PhD Candidate, "Carol I" National Defence University, Bucharest

Ghiță BÂRSAN, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Toma PLEȘANU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

In an alert, knowledge-based society, service and product quality plays an essential role in the success and survival of organisations in a competitive market.

In this article, we will briefly detail the implementation stages of the Quality Function Deployment (QFD) first phase – a global concept that provides means of transposing the requirements of clients (users) into the technical requirements appropriate for each stage of designing and creating a knowledge bank for defence, public order and national security.

In the first part, we will present a brief historiographical analysis of QFD, followed by the construction of the House of Quality (HOQ), the most commonly used matrix of all QFD components.

The results of the absolute and relative importance of the technical requirements following from the application of the steps of the house of quality will help the design team of the knowledge bank to implement with priority certain requirements of the potential users.

Keywords: house of quality, knowledge bank, customer requirements, technical characteristics.

INTRODUCTION

The quality of services and products plays an essential role in the success and survival of companies in a competitive market and this quality has a positive impact on customer loyalty to the company[1].

Implementing the quality function – Quality Function Deployment (QFD) is a global concept that offers means of transposing customer requirements into the technical requirements appropriate for each stage of the development and production of the desired products[2].

HISTORIOGRAPHICAL PRESENTATION OF THE QFD

The historiographical presentation of the QFD follows the directions identified by the researchers Lai-Kow Chan and Ming-Lu Wu in a study analysing about 650 publications, with references to the Internet, creating a reference bank on QFD organised in macro-areas[3].

The QFD Genesis

The quality implementation function is derived from six Chinese characters of Japanese Kanji writing *(Figure 1): Hin Shitsu (quality), Ki Nou (function), Ten Kai* (implementation). Japanese characters for *Hin Shitsu* represent quality, features or attributes, *Ki* and *Nou* represent function or mechanisation and *Ten* and *Kai* represent implementation, deployment, development or evolution. Taken together, the Japanese words mean *"the way we understand the quality our customers expect from us"*[4]. Therefore, the *"implementation of the quality function"* means that the responsibilities for producing a quality product must be assigned to all the component parts of a co-organisation[5].

[1] C. Jayawardhena, *The Impact of Service Encounter Quality in Service Evaluation: Evidence from a Business-to-Business Context*, in *Journal of Business & Industrial Marketing*, Vol. 25, No. 5, 2010, p. 338.
[2] L.P. Sullivan, *Quality Function Deployment,* in *Quality Progress* 19(6), 1986, pp. 39-50.
[3] L.K. Chan, M.L. Wu, *Quality Function Deployment: A Literature Review*, in *European Journal of Operational Research*, Vol. 143, 2002, pp. 463-497.
[4] M. Tottie, T. Lager, *QFD: Linking the Customer to the Product Development Part*, in *R&D Management*, vol. 25, 1995, pp. 257-267.
[5] Y. Akao, *Quality Deployment Including Cost, Reliability and Technology*, Quality, vol. 13, no. 3, 1983, pp. 61-77.

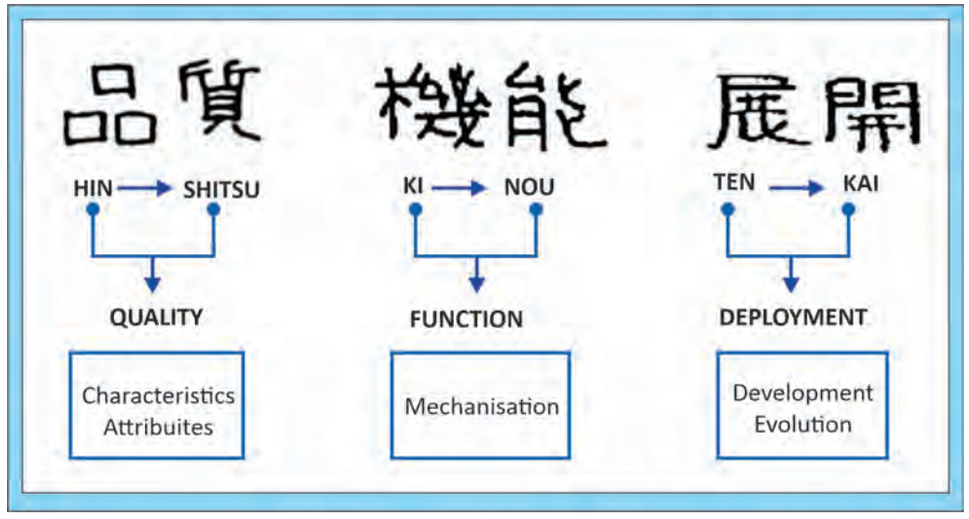


Figure 1: Translation of the six Chinese characters for QFD (adapted from Shahin)

The Art of Knowledge

QFD was developed in the late 1960s and early 1970s in Japan by professors Yoji Akao and Shigeru Mizuno, along with other quality experts. They wanted to develop a quality assurance method that took into account the customer satisfaction of a product before it was manufactured, aiming primarily at detecting possible problems during or after the manufacturing[6].

The Japanese industry began formalising QFD concepts in 1966, when a processing assurance chart was introduced at a Bridgestone Tire plant, which contained some of the main features of QFD[7].

The first certified works that encourage the concept of QFD were elaborated after several industrial studies in 1972 by Akao[8] and Nishimura[9].

QFD was introduced at Toyota Hino Motor in 1975 and Toyota Autobi in 1977. Due to the impressive results obtained from using QFD, this concept was later introduced to the entire Toyota group[10].

[6] *Idem*, *QFD: Past, Present, and Future*, Proceedings of the International Symposium on QFD, Linkping, retrieved on 31.05.2019, available at http://www.cadlab.tuc.gr/webmaster/06_QFD_PpF.pdf.
[7] A. Hill, *Quality Function Deployment*, in *Gower Handbook of Quality Management*, second edition, Gover, Brookfield, VT, 1994, pp. 364-386.
[8] Y. Akao, *New Product Development and Quality Assurance Deployment System* (in Japanese), in *Standardisation and Quality Control*, 25 (4), 1972, pp. 243-246.
[9] H. Nishimura, *Ship Design and Quality Table* (in Japanese), in *Quality Control* (JUSE) 23 (May), 1972, pp. 16-20.
[10] L.K. Chan, M.L. Wu, *op. cit.*, p. 465.

The first references to QFD penetration in US industries appeared after more than 10 years since the advent of QFD in Japan[11]. The first case study of QFD in the US was recorded in 1986, when Kelsey Hayes used QFD to develop a cooling sensor, which fully met the needs of customers[12]. The first US companies to include QFD in their production processes were: 3M, AT&T, Baxter Healthcare, Budd, Chrysler, DEC, Ford Motor, General Motors, Goodyear, Hewlett-Packard, IBM, ITT, Kodak Eastman, Motorola, NASA, Polaroid, Procter and Gamble and Xerox[13].

The influence of QFD also goes beyond the borders of Japan and the US, applications and studies of QFD being used in countries such as Australia, Belgium, Brazil, Denmark, Finland, Germany, Hong Kong, India, Ireland, Israel, Italy, Korea, Netherlands, Scotland, Singapore, Taiwan, Turkey and the United Kingdom.

THE STRUCTURE OF QFD

QFD is a method of developing the quality of the design that aims at consumer satisfaction and then the translation of the consumer's requirements into design objectives and quality assurance items that will be used throughout the entire production phase. It can be regarded as a process in which the consumer's voice is appreciated throughout the entire process of making products and services.

The basic elements of QFD are the following:

- determining customer requirements (EC).
- satisfying the way customers' requirements can be met (CUM) is essential for controlling the final product.
- the relationship between requirements and how they should be met.
- the target values corresponding to the requirements.
- the relationships between how the requirements are to be met.
- quantifying the importance of the requirements[14].

The QFD Phases

QFD uses several principles of competing engineering, where cross-functional teams are involved in all phases of product development, as shown in *Figure 1.2*. Each of the four phases of a QFD process uses a matrix to translate customer requirements from the initial planning stages through production control[15].

[11] M. Kogure, Y. Akao, *Quality Function Deployment and CWQC in Japan*, in *Quality Progress*, 16 (10), 1983, pp. 25-29.
[12] B. King, *Listening to the Voice of the Customer: Using the Quality Function Deployment System,* in *National Productivity Review* 6 (3), 1987, pp. 277-281.
[13] C. Adiano, A.V. Roth, *Beyond the House of Quality: Dynamic QFD*, in *Benchmarking: An International Journal*, 1 (1), 1994, pp. 25-37.
[14] P. Kumrawat, D. Verma, *Case Study of LMD & HD Trucks using Quality Function Deployment*, in *International Research Journal of Engineering and Technology*, vol. 4, no. 7, 2017, pp. 3159-3168.
[15] V. Bouchereau, H. Rowlands, *Methods and Techniques to Help Quality Function Deployment (QFD)*, in *Benchmarking: An International Journal*, vol. 7, no.1, 2000, pp. 8-19.

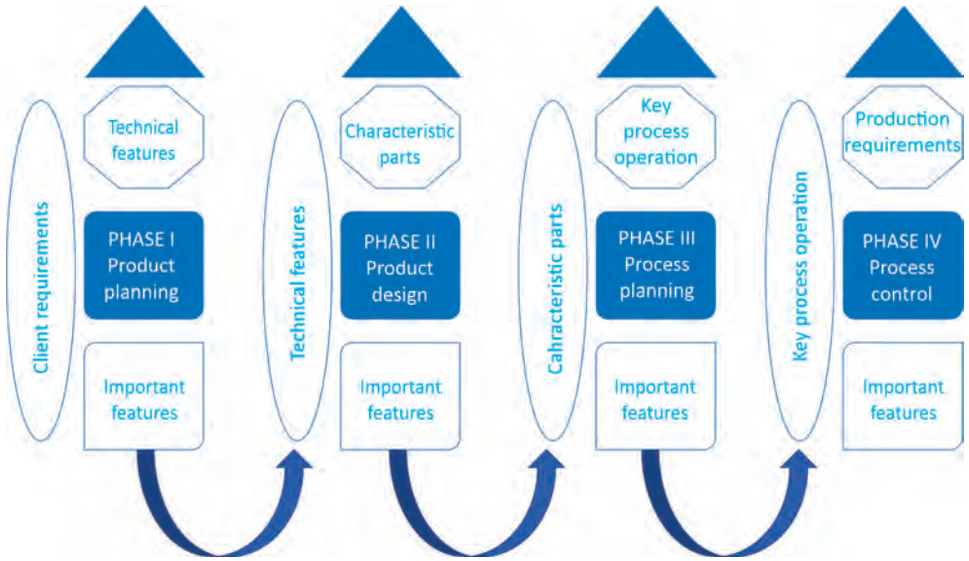


Figure no. 2: The four-phased QFD model (adapted after Bouchereau)

Each phase or matrix represents a specific aspect of the product requirements. The relationships between the elements are evaluated for each phase, and only the most important aspects of each phase are implemented in the following matrix.

The House of Quality corresponding to the field of defence, public order and national security

In order to capture a series of vital aspects for the planning process of the fulfilment of the knowledge bank for the field of defence, public order and national security (AOPSN), in the lines to follow, we will carry out the first phase of the QFD methodology, a composite matrix, hereinafter referred to as the House of Quality (HOQ). The basis of the HOQ is that the knowledge bank should be designed to reflect the requirements of customers (users). The focus in HOQ is on the correlation between client needs (EC), and engineering characteristics (CUM). According to Hauser and Clausing, the house of quality is *"a kind of conceptual map that provides the means for planning and cross-functional communication"*[16].

Next, we will present the achievement of the house of quality for the above-mentioned knowledge bank. This matrix transforms the requirements of the clients, based on the results of the research of a pilot study and the data obtained

[16] J. R. Hauser, D. Clausing, *The House of Quality*, Harvard Business Review, May-June 1988, pp. 63-73.

from the application of an online questionnaire[17], into an adequate number of engineering targets that must be met by the knowledge bank for the AOPSN.

The process of designing the questionnaire took place within a focus group, which took into account the answers to a set of questions addressed to decision-makers from several structures of the Ministry of Internal Affairs. An important aspect referred to as whether respondents were aware of various notions used in building up the knowledge bank, reaching all aspects related to the state of knowledge in the field of organisational learning[18]. The house of the quality matrix for the knowledge bank we have posted on the Google Drive application storage corresponding to the knowledge bank address: *bancadecunostinte@gmail.com*, using the password: *banca.de.cunostinte*[19].

Step 1: List of customer requirements (EC)

The requirements of the users (the voice of the client) according to the answers received in the online questionnaire and of the focus group are the following:

- to search once for more keywords;
- to be user-friendly;
- data security;
- restricted access;
- to allow the search for knowledge in a particular field;
- personal data protection;
- providing the security conditions of the documents;
- how can I be up to date with the new works added?
- how can I be up to date with the most accessed works?
- where do we find out which works are most sought after?
- how can I get in touch with the platform administrator as soon as possible?
- can I download a paper that interests me?
- the introduction of a new document to appear in the RSS feed;
- the response time of the website on which the application runs to be as short as possible;
- the website hosting the platform to adapt its page design according to the viewing environment (screen resolution at: desktop, laptop, tablet, phone);
- fault tolerance and fault recovery.

Step 2: Evaluate the importance of the requirements by the customers

On a 1 to 5 scale, potential users evaluate the importance of each requirement. This value will be used later in the relationship matrix.

[17] https://docs.google.com/forms/d/e/1FAIpQLSdJ9afVLRiGyCZWVQysP8LI-OVqwiC8JRa4DGaOZXNUe69d1g/viewform

[18] R. M. Oanță, *Procesul implementării lecțiilor învățate la nivelul Ministerului Afacerilor Interne*, Buletinul Universității Naționale de Apărare "Carol I", no. 2, București, 2019, pp. 56-62.

[19] https://docs.google.com/spreadsheets/d/11DR2D4hsez_1dVEjVy9JFdRuxpxUTfw9PXG-b6zHzjY/edit#gid=929470925

Step 3: Competitive evaluation by customers

Possible users of the knowledge bank for the AOPSN domain assess the importance of the requirements from ***step 2*** in relation to the knowledge banks resulting from applying the online questionnaire through the Google Forms platform: Ohio Knowledge Bank, NATO LL Library, Plantwise Knowledge Bank, Sea Knowledge Bank.

Step 4: List of technical characteristics (CUM)

The technical characteristics (voice of the engineer) or the technical descriptors are attributes of the knowledge bank for the AOPSN domain that can be measured and evaluated against competitors.

- the knowledge bank platform should have the advanced search function;
- friendly interface with an attractive design;
- security policies are implemented on the server where the platform is hosted;
- access to the platform is based on the user and password;
- sorting data after a search is done by relevance, date, title, ascending and descending;
- implementation of GDPR measures. Notifying users about the processing of personal data;
- the terms and conditions section;
- the recently added section;
- the records of the accesses;
- the most wanted section;
- live chat window, contact section, email phone;
- each work has a download section;
- the website on which the application runs has an RSS feed;
- the processing speed of the request;
- the design of the website on which the application runs is of web responsive type;
- replication of data and services on multiple servers.

Step 5: Directions for improvement

After defining the technical descriptors, it is determined the direction in which each descriptor (maximisation, minimisation, or stagnation) must move.

The following technical descriptors should be maximised:

- the knowledge bank platform to have the advanced search function;
- friendly interface with an attractive design;
- access to the platform is based on the user and password;
- sorting data after a search by relevance, date, title, author, ascending and descending;

- each work has a download option;
- the processing speed of the request;
- replication of data and services on multiple servers.

Step 6: Relationship Matrix (between EC and CUM)

With the help of the relationship matrix, the relationship between the client requirements and the organisation's ability to meet them is determined. The relationship between the technical descriptors and the requirements of the clients can be strong, moderate or weak, represented by the symbols ●, ○ or ▽, which correspond to the numerical values 9, 3 or 1.

The strong relationships between technical descriptors and customer requirements are represented in the table below:

Table no. 1: Strong relationships between technical descriptors and customer requirements

What needs to be done? (The client's voice)	**How should it be done? (The engineer voice)**
To search using several keywords at once	The Knowledge Bank platform should have an *advanced search* function.
	Friendly interface with an appealing design.
	Search sorting by relevance, date, title, author, ascending and descending.
User-friendly	The Knowledge Bank platform should have an *advanced search* function.
	Search sorting by relevance, date, title, author, ascending and descending.
Secure data	Security policies should be implemented on the server where the platform is housed.
	The platform access should be done by means of a user and a password.
Restricted access	The platform access should be done by means of a user and a password.
To allow knowledge searching in a certain field	Search sorting by relevance, date, title, author, ascending and descending
	The Knowledge Bank platform should have an *advanced search* function.
Personal data protection	Implementing GDPR measures. Informing users about GDPR.
Document security prevention	The terms and conditions section.
How can I keep up to date with recently added papers?	The recently added section.

What needs to be done? (The client's voice)	How should it be done? (The engineer voice)
How can I be up to date with most frequently accessed papers?	Keeping track of accessing.
How can I learn where the most frequently searched papers are?	The *most wanted* section.
How can I get in touch with the platform administrator as shortly as possible?	Live chat window. Contact, phone number and email.
How can I download a paper I am interested in?	Each paper should have a download section.
	The speed of request processing.
Introducing a new document should be through RSS feed	The website on which the application runs should have RSS flux.
The response time lap of the website on which the application runs should be as short as possible	The speed of request processing.
	Data and service replication on several servers.
The platform website should adapt the page design depending on the viewing environment (the desktop's, laptop's, tablet's or phone's monitor resolution)	The website design on which the application runs should be of a responsive web type.
Error tolerance and retrieval	Data and service replication on several servers.

Moderate relationships between technical descriptors and customer requirements are represented in the table below:

Table no. 2: Moderate relationships between technical descriptors and customer requirements

What should be done? (The client's voice)	How should it be done? (The engineer voice)
User-friendly	A friendly interface with an appealing design.
	The *most wanted* section.
	The website design on which the application runs should be of a responsive web type.
Secured data	Implementing GDPR measures. Informing users about GDPR.
	The terms and conditions section.
Restricted access	Security policies should be implemented on the server where the platform is housed.

What should be done? (The client's voice)	How should it be done? (The engineer voice)
Protected personal data	Security policies should be implemented on the server where the platform is housed.
	The platform access should be done by means of a user and a password.
Document security prevention	Security policies should be implemented on the server where the platform is housed.
How can I be informed about the newly added papers?	The website on which the application runs should have RSS flux.
	Search sorting by relevance, date, title, author, ascending and descending.

Step 7: Organisational Difficulty

On a scale from 1 to 5, the project team (engineers) evaluate the design attributes in terms of organisational difficulty. Certain design attributes may be in direct conflict with organisational policies.

Step 8: Technical analysis of competitors' products

A comparison was made by the technical specialists (the engineering team) between the technical descriptors of the knowledge bank and those of the competitors, the same as in ***step 3***.

Step 9: The correlation matrix between the pairs of CUM or the correlation matrix of the technical descriptors

The matrix of interrelation between pairs of CUM (also called the *"roof"* of the House of Quality) examines the impact of the technical descriptors on each other. The correlations are represented by mathematical symbols that indicate a positive (+) or a negative (-) correlation. The lack of a correlation between the requirements is represented by "". The project team examines the impact of the technical descriptors on each other.

The technical descriptors among which there is a positive correlation are presented in the following table:

Table no. 3: Technical descriptors among which there is a positive correlation

Technical Descriptor	Technical Descriptor
The Knowledge Bank platform should have an *advanced search* function.	Friendly interface with an appealing design
	Search sorting by relevance, date, title, author, ascending and descending.
	Request processing speed

Technical Descriptor	Technical Descriptor
Friendly interface with an appealing design	Each paper should have a download section.
	The website design on which the application runs should be of a responsive web type.
	Live chat window. Contact, phone number and email.
Security policies should be implemented on the server where the platform is housed.	The platform access should be done by means of a user and a password.
	Implementing GDPR measures. Informing users about GDPR.
The platform access should be done by means of a user and a password	The terms and conditions section.
Implementing GDPR measures. Informing users about GDPR	The terms and conditions section.
Search sorting by relevance, date, title, author, ascending and descending.	Application processing speed
	Data and service replication on several servers.
The recently added section	Records of the accesses
	The website on which the application runs should have RSS flux.
Each work has a download section	Data and service replication on several servers.
Application processing speed	Data and service replication on several servers.

Step 10: The absolute and relative technical importance

The numerical value of the absolute technical importance is obtained by summing on the column (for each technical descriptor) the product between the value of the cell and the value of the importance evaluated by the customers.

The relative importance (%) is obtained by summing the values of the technical descriptors and then dividing the value of each technical descriptor by the respective sum. Thus, it is to be known which of the technical aspects matters most to clients. The hierarchy of the technical descriptors by importance can be found in the table below.

Table no. 4: The abso.lute technical and relative importance of technical descriptors

No.	Technical descriptor	Assessment of the technical importance	Relative importance
1.	Search sorting by relevance, date, title, rising and falling	229,69	14%
2.	The *advanced search* function	210,94	13%
3.	User access and password	164,06	10%
4.	Implementation of security policies	140,63	9%
5.	Friendly interface	93,75	6%
6.	Implementation of GDPR measures	93,75	6%
7.	Section terms and conditions	93,75	6%
8.	Application processing speed	84,375	5%
9.	Responsive web design	79,69	5%
10.	Recently added section	70,313	4%
11.	Voting system for each work uploaded	65,625	4%
12.	RSS Feed	65,625	4%
13.	Most wanted section	56,25	4%
14.	Download option for each work	56,25	4%
15.	Live chat window. Contact section	42,188	3%
16.	Replication of data and services	42,188	3%

CONCLUSIONS

QFD is a structured process, a set of engineering and management diagrams interconnected with each other, with which, based on the client's requirements, the characteristics of the design and production processes are realised. Therefore, QFD is oriented towards involving a team of individuals from different departments working in product development: marketing, design, quality assurance, manufacturing, financial accounting.

In conclusion, QFD can be defined as a method of developing the design that aims to satisfy the needs of the clients, trying to translate the client's requirements into design objectives, with the mention that these requirements will be met in the production stage only with the help of quality assurance methods. Thus, QFD can be briefly defined as product development based on customer requirements.

Of the 4 phases of QFD, the most important is the first, namely the house of quality, which gives us important considerations for the design, planning, manufacturing and testing processes.

At the "Structure of QFD" subtitle, we have detailed all the aspects related to the house of quality for the knowledge bank in the field of AOPSN. The initial steps in forming the house of quality include determining, clarifying and specifying the needs of the users, which are more precisely called the voice of the client. Once the needs and expectations of the customers have been identified, they must be included in the technical specifications of the products, nothing being designed, made or produced without having detailed technical specifications. These characteristics are expressions of the client's voice translated into a technical language, so-called the engineer's voice. We must mention that the list of technical characteristics can be structured hierarchically, on several levels. The relationship matrix offers a comparison between customer requirements and technical characteristics, the number of comparisons being based on the number of customer requirements and the number of technical characteristics. Having in mind this overall customer image, the organisation can begin to formulate a product improvement strategy.

The technical correlation matrix, also called the HOQ roof, is used to develop relationships between customer requirements and product requirements. This matrix allows the team of engineers to discover which are the most important of the technical characteristics.

The planning matrix shows the weighted importance of each requirement that the project team and its competitors are trying to meet.

The prioritisation of the technical characteristics is realised with the help of the calculation algorithms, taking into account the technical characteristics based on the matrix of relations, the prioritised requirements of the clients and the matrix of interrelation.

The final output of the matrix is a set of target values for each technical requirement that must be met by the knowledge bank for the AOPSN domain, the first ranked technical descriptors being the following:

- sorting upon search by relevance, date, title, ascending and descending;
- advanced search function;
- password and user access;
- implementation of security policies.

Although the technical descriptor *replication of data and services on several servers* was ranked last, we consider that in order to achieve the sustainability of the knowledge bank, this aspect must be considered, being very important in case of disaster.

BIBLIOGRAPHY

1. C. Adiano, A. V. Roth, *Beyond the House of Quality: Dynamic QFD*, in *Benchmarking: An International Journal*, 1 (1), 1994.
2. Y. Akao, *New Product Development and Quality Assurance Deployment System* (in Japanese), in *Standardisation and Quality Control*, 25(4), 1972.
3. Y. Akao, *QFD: Past, Present, and Future*, Proceedings of the International Symposium on QFD, Linkping, http://www.cadlab.tuc.gr/webmaster/06_QFD_PpF.pdf.
4. Y. Akao, *Quality Deployment Including Cost, Reliability, and Technology*, in *Quality*, vol. 13, no. 3, 1983.
5. V. Bouchereau, H. Rowlands, *Methods and Techniques to Help Quality Function Deployment (QFD)*, in *Benchmarking: An International Journal*, Vol. 7, No. 1, 2000.
6. L. K. Chan, M. L. Wu, *Quality Function Deployment: A Literature Review*, in *European Journal of Operational Research*, vol. 143, 2002.
7. J. R. Hauser, D. Clausing, *The House of Quality*, in *Harvard Business Review*, May-June 1988.
8. A. Hill, *Quality Function Deployment*, in *Gower Handbook of Quality Management*, second edition, Gover, Brookfield, VT, 1994.
9. C. Jayawardhena, *The Impact of Service Encounter Quality in Service Evaluation: Evidence from a Business-to-Business Context*, in *Journal of Business & Industrial Marketing*, vol. 25, no. 5, 2010.
10. B. King, *Listening to the Voice of the Customer: Using the Quality Function Deployment System,* in *National Productivity Review* 6 (3), 1987.
11. M. Kogure, Y. Akao, *Quality Function Deployment and CWQC in Japan*, in *Quality Progress* 16 (10), 1983.
12. P. Kumrawat, D. Verma, *Case Study of LMD & HD Trucks using Quality Function Deployment*, in *International Research Journal of Engineering and Technology*, vol. 4, nr. 7, 2017.
13. H. Nishimura, *Ship Design and Quality Table* (in Japanese), in *Quality Control* (JUSE), 23 (May) 1972.
14. R. M. Oanță, *Procesul implementării lecțiilor învățate la nivelul Ministerului Afacerilor Interne*, Buletinul Universității Naționale de Apărare "Carol I", nr. 2, București, 2019.
15. R.M. Oanță, T. Pleșanu, *Knowledge Sharing – The First Step towards Building up a Knowledge Bank*, the 14th International Scientific Conference *"Strategies XXI"*: *Strategic Changes in Security and International Relations*, București, 2018.
16. L. P. Sullivan, *Quality Function Deployment,* in *Quality Progress* 19(6), 1986.
17. M. Tottie, T. Lager, *QFD: Linking the Customer to the Product Development Part*, in *R&D Management*, vol. 25, 1995.

THE USE OF TANKS IN MAIN MILITARY CONFLICTS

Nicolae PLEŞANU
PhD Candidate, "Carol I" National Defence University, București

Ghiță BÂRSAN, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Sorin-Gheorghe PÎNZARIU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Since appearing on the battlefield, in less than a decade, tanks have revolutionised the art of war. This article focuses on the use of tanks from the beginning to nowadays. We will showcase some battles in which the tanks were used, in the First World War, in the Campaigns of East, West and North Africa of the Second World War and the conflicts of the last decades.

Keywords: tank, battle chariot, fast war, campaign, blitzkrieg.

INTRODUCTION

The use of tanks on the battlefield would not have been possible without the technological discoveries of the late 19th and early 20th centuries, especially those regarding the energy aggregate, the propeller (track) and the protection (shield).

Compared to other weapons, the tank was the fastest developing weapon system in the history of war. The assessments of the impact produced by the use of tanks in the whole army were accompanied by predictions of some military specialists who anticipated changes of the operational concepts.

The design and construction of the tank appeared as a necessity to solve an unusual tactical situation, namely the deadlock in the trenches of the First World War. Basically, this means of attack was created to break the defence, the protection of the infantry and to reduce the importance of the machine gun on the battlefield.

THE APPEARANCE OF TANKS AND THEIR USE IN THE FIRST AND SECOND WORLD WAR

Until 1916, the First World War remains a trench warfare, essentially static, in which the concept of linear defence of the *"tactical slaughter"*[1] type was adopted.

In the famous battle on the Somme River, recognised as the bloodiest of the First World War with a total of 1,200,000 dead and wounded on both sides, the tank was used for the first time by the British.

The name "*tank*" was given by the British to keep the real purpose of the first models secret when they were transported to France, announcing that they would be used as water tanks.

The First World War

On 15 September 1916, in the area of Fleurs – France, the British used a tank model named "Mark I", which entered service in August 1916. It was produced in two versions, "man" and "woman", 28 tons, respectively 27 tons, with different masses due to the different weapon equipment (the woman tank was only equipped with machine guns). Both models had a crew of 8 soldiers, a shield of 12-15 millimetres and were not equipped with a turret or with noise mitigation devices produced by the engine. Of the 32 tanks used, only a third were able to break the defence,

[1] K.H. Frieser, *Mitul Blitzkrieg-ului, Campania din Vest a Wehrmacht-ului 1940*, Editura Militară, București, 2010, p. 353.

some were damaged before entering the battle and others were removed from the battle by the German artillery[2]. The result so far had been favourable to the attackers, the use of tanks producing devastating effects on German morale. Although the engagement of the tank in combat did not change the static character of the war, its potential was discovered and the nature of the future wars has never been the same. Used on a wider front, their effectiveness was limited, considering that at that time the infantry had little training in dealing with tanks and the strategies of those times did not trust these armoured monsters as they considered them fanciful and unusable weapons. As a result, the infantry acted independently of the tanks, which allowed the German infantry to repel the attack.

In April 1917, a large-scale battle took place on the northeast front, near the French town of Bery au Bac. A total of 132 Schneider tanks, built in France, went on the offensive, the adopted fighting disposition being one in line. But same as in the case of the first British tank attack, the French offensive was a failure that resulted in the loss of more than half the tanks.

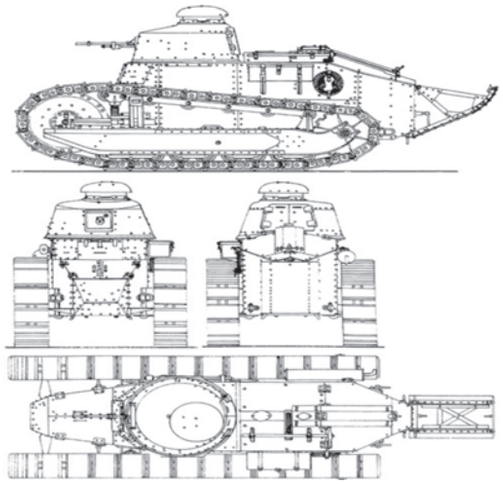


Figure no. 1: The tank Renault FT-17, 8 mm, 1917[3]

The first large-scale engagement of tanks in combat took place on 20 November 1917. In an attack on Cambrai, about 400 tanks broke the German defence and penetrated the depth of their disposition about 10 kilometres on a front of approximately 11.3 kilometres. Unfortunately, this time, the success was not complete, because it was not possible to exploit and maintain the land gained by using tanks[4] due to the operational concepts used by the strategies of those

[2] http://www.army-technology.com/features/featuretimeline-100-years-of-tanks-5694455/.
[3] https://www.the-blueprints.com/blueprints/tanks/tanks-r/72310/view/renault_ft-17_8mm_1917/.
[4] https://www.globalsecurity.org/military/systems/ground/tank-history1.htm.

periods. Charles Fuller[5] observed, in the battle of Cambrai, the effect of the tank on the morale of the military and that the terror caused by it and not the destructive effects led to the defeat of the German forces[6].

France was the country that built a tank similar to the ones that are used today, introducing between 1916-1917 the turret on the model *"Renault – F.T. 1917"*, (equipped with a 37 mm cannon and machine gun), model that remains a technical reference of the tank with a 360-degree rotary turret. The tank Renault – F.T. 1917 is presented in *figure no. 1* and its characteristics in *table no. 1*.

Table no. 1: The main characteristics of the light tank Renault FT 17 (France)[7]

TECHNICAL CHARACTERISTICS	
Type	Lightweight tank
Length	4,95 m
Width	1,71 m
Height	2,14 m
Crew	2 people
Weight	6, 7 tons
Radio equipment	-
WEAPONS	
Main armament	37 - mm caliber cannon or 8 mm caliber machine gun
Turret rotation	360º
MOBILITY	
Motor	Internal combustion Renault, 4 cylinders petrol, cylinder capacity 4.48 L, liquid cooled, with a power of 35 HP
Transmission	4 gears
Effective	Maximum speed 7,5 km/h, maximum distance that could be travelled with fuel from the reservoir 35 km
Total number constructed: From 1918 until production is removed	3,750 pieces

[5] Military historian and British strategist, a theorist of modern armoured warfare.
[6] J.F.C. Fuller, *The Decisive Battles of the Western World and their Influence upon History*, vol. III, Eyre & Spottiswoode, London, p. 279, apud Major J.G. Pierre Lamontagne, *Are the Days of the Main Battle Tank Over?*, Master of defence studies, Canadian Forces College, CSC 29/CCEM N29, available at https://www.cfc.forces.gc.ca/259/290/289/286/ lamontagne.pdf.
[7] http://www.chars-francais.net/2015/index.php/engins-blindes/chars?task=view&id=688.

The name given by the French to the tanks of those times was "*fighting car*" or "*assault car*" and thus one could determine the role that they would have on the battlefield, namely the conquering of a fortified place, an objective or to break the enemy's resistance by a decisive attack.

Germany reacted quickly through a tank design and production programme. The first model was named A7V, weighing 30 tons and a crew of eighteen people. By the end of the war, due to the lack of raw materials, about twenty such tanks were built.

It is considered that the first direct confrontation involving two battle tanks took place on 24 April 1918, near Villers-Bretonneux, between a German A7V and an English Mark IV. This fight was neither won nor lost because both tanks were equipped with machine guns only[8].

Numerous mechanical failures and vulnerability in the case of tanks not accompanied by infantry and ground attack aircraft, in order to locate and neutralise the anti-tank defence cast doubt on the usefulness of tanks.

Almost three years after the use of tanks on the battlefield, on 1 August 1919, in the Mihai Bravu garrison, it was established the first battalion of our country. This battalion consisted of four light-fighting companies and a repair company (fixed and mobile workshop)[9]. It was equipped with French light tanks Renault – F.T. 1917, from their terminology used by the French, resulting the name „*battle chariots*" of the battalion.

The interwar period

After the First World War, two schools emerged from the strategies of those times:

- a conventional school that considered that the tank was only a vehicle to accompany the infantry, to support the important role in carrying out the combat actions being of the infantry. At that time, the management of the military structures was predominant among the infantry officers;
- a progressive school in which some advocates, Estienne[10], then de Gaulle[11] in France, Guderian[12] in Germany, Fuller in England and Tuhacevski[13] in Russia (Soviet Union), proposed using tanks in conjunction with aviation. The suggestions of these officers were successfully applied by Germany since September 1939.

[8] http://www.globalsecurity.org/military/systems/ground/tank-history1.htm.
[9] Asociația culturală "Valeriu Florin Dobrinescu", *Armata română și evoluția armei tancuri. Documente (1919-1945)*, Editura Universității de Stat din Pitești, Pitești, 2012, p. 16.
[10] Jean Baptiste Eugène Estienne, French General, considered the father of the tank weapon in France.
[11] Charles de Gaulle, French General and politician.
[12] Heinz Wilhelm Guderian, General and military theoretician of the German army.
[13] Mihail Nicolaevici Tuhacevski, Marshal of the Soviet army.

In the mid-1920s, German General Guderian made public in a specialised work an operational concept, consisting of the massive use of tanks as a shock force, in cooperation with fighter planes. Thus, the foundations of a new concept were laid, called Blitzkrieg during the Western Campaign, a synonym for "*operative movement warfare*" [14].

During the 1920s and early 1930s, due to the limited role assigned to tanks by commanders of infantry structures, as well as budgetary constraints, the development of tanks was slow. Many nations did not consider the lessons learned from the First World War and did not foresee the importance that tanks would have on the future battlefield. Thus France, England and the US were part of these nations claiming that those years of the great war were an aberration in military development. In contradiction, in Germany and Russia, the use of tanks in carrying out military actions has become a subject of thorough study, a group of military specialists from these countries predicting the place held by the tank within the mechanised forces that would be used to carry out rapid actions[15].

After the First World War, the French Renault – F.T.17 tank remained for a long time a technical reference. The Renault factory would also develop other D1 and D2 tanks between 1931-1933 and especially R.35 in 1935, a true successor of F.T.17.

In England, the development of light tanks, used to maintain order in India (where they had to be transported), was favoured to the detriment of medium and heavy tanks.

In Germany, the stipulations of the Versailles Treaty of 1919 prohibited the production of tanks. The progressive re-equipping of the Armed Forces (Wehrmacht) was done, starting with 1933, with the violation of the treaty, with tanks Panzer I, II and III whose mass ranged from 6 to 23 tons.

In the USA, the interwar period was marked especially by the emergence of a genius named J.W. Christie, an American car engineer, who developed a suspension system that allowed tanks to achieve speed performance. Because the US Army broke the contract with engineer Christie, he exported his ideas to Russia. Thus, using Christie's design and production techniques, Russia built, between 1929-1940, an extremely reliable and balanced tank called the T-34, which became the main combat tank of the Red Army in the Second World War.

The Second World War

Compared to the First World War, a static, trench warfare, in the second world conflagration, the strategy was oriented towards a fast, decisive result. The German army sought to use the maneuver of the forces, resulting in the concepts "*quick*

[14] K.H. Frieser, *op. cit.*, p. 4.
[15] http://www.encyclopedia.com/social-sciences-and-law/political-science-and-government/military-affairs-nonnaval/ military-tank.

war" and "*short war*"[16]. This way of conducting the operative manoeuvre war received the name of blitzkrieg, defending, at that time and later, many theories about this concept.

Hitler ordered the attack on Poland, convinced that France and England would not dare to respond with war. The two great powers did not react: in 1935, when the compulsory military service was reintroduced in Germany; in 1936 when German forces entered the demilitarised area of Rhineland; in 1938, when Germany annexed Austria and transferred the regions of Czechoslovakia inhabited by the Germans as well as in March 1939, when the other regions of Czechoslovakia were invaded. But, three days after the attack on Poland, on 3 September 1939, the Second World War broke out through a declaration of war by France, England and, immediately thereafter, the Commonwealth states.

In the Polish campaign, the Germans used a new operational concept for the first time, the use in combat of tanks supported by aviation. This campaign represented the field of experimentation of this new concept which had not been tested before in military exercises. Germany's success came quickly, less than a month after the attack began, because Poland was attacked by Russia on 17 September 1939, and thus divided between Germany and Russia. Compared to the Western Campaign, tank structures were not used as independent, large-scale, operational forces, they were fighting only at the tactical level within the divisions[17].

At the beginning of the war, Germany had prepared a plan of operations against Poland but had no plan for a confrontation with the Western powers. If France had attacked Germany upon declaring war, exploiting the engagement of German forces in Poland, "*it could have crossed the Rhine, without us being able to prevent it, and threaten the Ruhr Basin, the most important factor in leading the war by the Germans*" declared a German General after the war ended[18].

The Polish campaign was not over when Hitler, on 27 September 1939, announced that he had decided to attack the Western powers. A provisional term was set for the attack, on 25 November 1939, which was postponed 29 times, until 10 May 1940, when the Western Campaign began.

Military analysts consider that the seven months between the Polish and Western campaigns were the time interval that the German army needed for technical procurement and units training.

[16] K.H. Frieser, *op. cit.*, p. 364.
[17] *Ibid*, p. 42.
[18] *Ibid*, p. 39.

Table no. 2: Structures of forces and technical means of combat used in ground and air[19]

Forces and technique / Countries	Divisions	Number of military land forces	Tanks	Cannons	Aircraft
Germany	135 (of which 10 tanks and 42 reserve)	3,000,000	2,439	7,578	3,578
The Allies, France, England, Belgium and the Netherlands	151	Aprox 4,000,000	3,254	14,000	4,469

Germany and the allies, France, England, Belgium and the Netherlands, used for the West offensive, the structures of forces and technical means of combat used in the ground and air battles mentioned in *table no. 2*[20].

As you can see, there was a relatively numerical balance between the combat forces, but a quantitative and qualitative comparison of the technique tilted the balance in favour of the allies to most weapons systems.

It was demonstrated during the campaign for France in 1940 that, in a war, the doctrinal concepts and training of the military can often compensate for deficiencies in terms of both quality and quantity of equipment. Although the French tanks were more numerous than those of the Germans and, for the most part, were equipped with larger calibre guns and thicker armour, they did not cope with the German concept of warfare.

One lesson of the First World War that was not fully learned at the time was that tanks can only really be effective when they concentrated in large numbers on favourable ground and received fire and adequate logistical support.

The Battle of Hannut, on 12-13 May 1940, is considered the first and largest tank battle of the Western Campaign. With all the quantitative superiority (ratio 415 to 125) as well as the quality of the French tanks over those of the Germans, the rigid tactics and the preference of the French commanders for the linear arrangement of the units, specific to the First World War, led to the loss of the battle and their withdrawal. A tactical advantage was given to the Germans by aviation, which supported the action of ground forces. Another technical advantage was the provision of all tanks with radio stations that allowed the German

[19] Adaptation from K.H. Frieser, *op.cit.*, p. 77.
[20] *Ibid*, pp. 58-77.

commanders a permanent leadership of the forces, respectively changing the direction of concentration of efforts.

Another tank battle, during the Western campaign, took place at Flavion on 15 May 1940. The force report was clear in favour of the French, which had 170 tanks while the Germans only 30 tanks, of the Panzer III types and IV (modern) and 90 Panzer I and II types, which could not be used in the battle with the opposing tanks due to the low firepower[21] (these being equipped with two twin machine guns - Panzer I - and a 20 mm cannon and a machine gun half - Panzer II). The advantage of equipping each German armoured vehicle with radio stations and fire support from aviation and artillery, as well as the impossibility of fueling the French tanks, led to the destruction of a French division.

As a result, the invasion of the Netherlands and Belgium, as well as the attack from Sedan, with German spearhead tank divisions, permanently supported by large numbers of aircraft and artillery, made the Allied armies, commanded in the manner of the First World War, to be very easily overcome, although numerically they were of the same value and were in defense.

General Gamelin, the supreme commander of the French army, would have mentioned in front of Churchill the three reasons for his army's defeat in Sedan: "*numerical inferiority, procurement inferiority, tactics inferiority*"[22]. From the ones presented above, we can say that only the third reason is valid.

The campaign in the West ended unexpectedly quickly for the Allies, who capitulated in order, as follows: May 15 Holland, May 27 Belgium and 21June 1940 France.

Following the unexpectedly rapid success of the West, on 22 June 1941, Germany, together with the allies Romania, Finland and Hungary, launched the attack on Russia (Soviet Union), wishing that the duration of this campaign would be only three months.

With the start of the operation Romania enters the Second World War, having constituted, from March 1941, the 1st Armored Division "Great Romania", which had the following composition:

Division headquarter;

- 3rd Motorised Hunters Regiment;
- 4th Motorised Hunter Regiment;
- 1st Motorised Artillery Regiment;
- 1st Fighting Cars Regiment;
- 2nd Fighting Cars Regiment;
- 1st Motorised Specialties Battalion;
- 1st Engineers Motorised Battalion;

[21] *Ibid*, p. 261.
[22] *Ibid*, p. 78.

- 1 pioneers battalion;
- 1 special armament battalion;
- 1 signal company[23].

This division consisted of 200 tanks (which were fighting) out of the total 374 of the Romanian Army[24]. As is known, the decision to participate in our country was taken in the context of Russia's occupation of Basarabia on 23 August 1939, by the non-aggression treaty concluded between Russia and Nazi Germany, the Ribbentrop-Molotov Pact, also known as the Stalin-Hitler Pact.

The successes of the first months of the campaign created the sensation of a quick victory over Russia, which lost many large units in encirclement battles (nearly four million servicemen) by December 1941. The cold winter of 1941 stopped the offensive against Russia.

For this campaign, the German tanks had a remarkable development to face the adverse tanks. Hitler demanded the construction of a heavy tank Panzer VI (Tiger I) which was sent to the Russian front, in Leningrad, in 1942. To face the T-34 tank, Panzer V (Panther) tanks were built. The increase in the protection by the increase in the shield with the effect of increasing the weight, continued until the end of the war with the appearance of the tank of Königstiger (Tiger Royal) of 68 tons and various prototypes until the huge Mauss with a mass of 189 tons. But as a result of the lack of raw materials, the number of tanks made by Germany was reduced compared to the number made by Russia and its allies due to economic superiority and technological simplicity.

The introduction of new technical means on the battlefield of the First World War showed that it was conditioned by the industrial production capacity of the belligerent nations and their material resources. Thus, nations with a high production capacity of technical and resource-rich means of supporting a war have a decisive advantage in the event of a prolonged conflict.

In *Figure no. 2* it is shown the industrial production in the number of tank units built, between 1939-1945, by the main countries involved in the conflict[25].

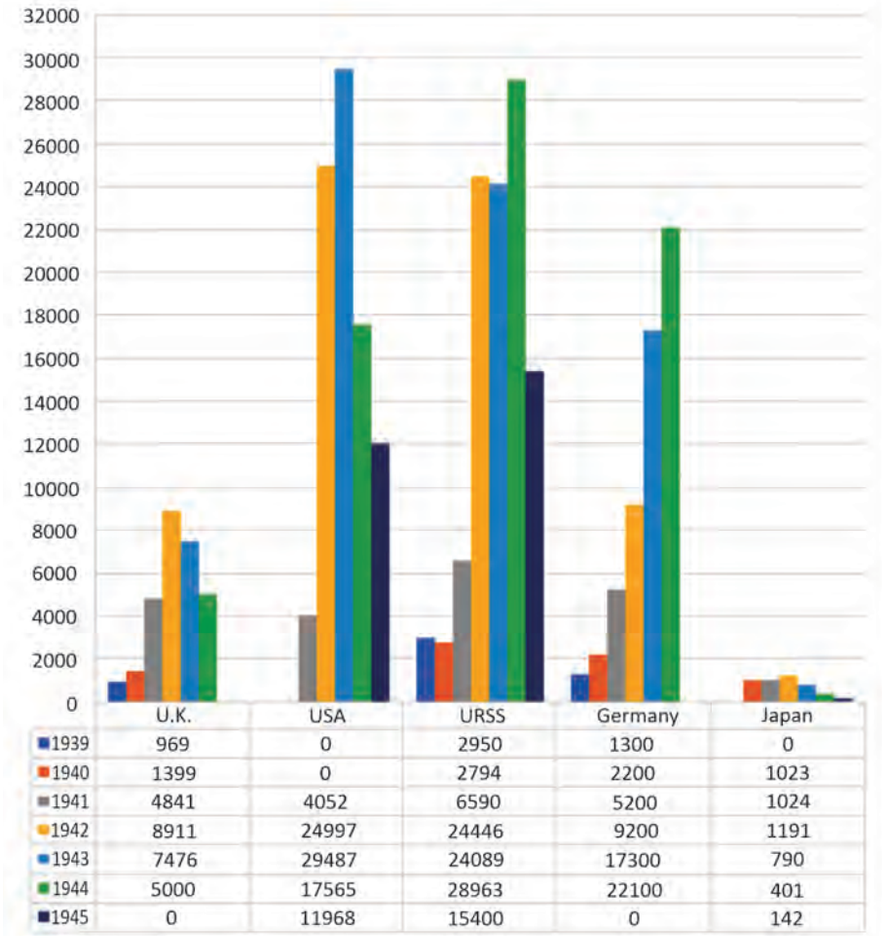
You can easily see the high production capacity of Russia (USSR) and the US, which had the most units built between 1942 and 1945.

The biggest tank battle in history took place in the area of Prokhorovka (Russia) on 12 July 1943, as part of the Kursk Battle (from 5 July to 23 August 1943)[26].

The Battle of Prokhorovka brought more than 1,200 tanks in the field, of which about 450 Germans. The losses in terms of tanks were not established exactly

[23] Asociația culturală „Valeriu Florin Dobrinescu", *op.cit.*, pp. 63-64.
[24] *Ibid*.
[25] *Ibid*, p. 88.
[26] https://www.historia.ro/sectiune/general/articol/un-mit-al-propagandei-sovietice-kursk-1943-cea-mai-mare-batalie-de-tancuri-din-istorie.

but the strategic result was clearer. The success of the Russians from the summer of 1943 was due to the superiority in the number of troops and means of fighting, as well as in the preparation of the ground and the forces for defence. Because the Russian intelligence services found out about the German offensive plan, the attack missed the element of surprise.



	U.K.	USA	URSS	Germany	Japan
1939	969	0	2950	1300	0
1940	1399	0	2794	2200	1023
1941	4841	4052	6590	5200	1024
1942	8911	24997	24446	9200	1191
1943	7476	29487	24089	17300	790
1944	5000	17565	28963	22100	401
1945	0	11968	15400	0	142

Figure no. 2: Tank production from 1939-1945[27]

Tanks also played an important role in North Africa in the second battle of El Alamein, which took place between 23 October and 5 November 1942. This was the first major victorious allied offensive against the Germans in which about 1,600 tanks were involved, of which more than 500 were Germans and Italians.

[27] Spencer C. Tucker, *Weapons and Warfare Series, Tanks, An Illustrated History of their Impact*, ABC-CLIO, Inc., 2004, ABC-CLIO, Inc., 2004, p. 88.

USE OF TANKS IN MILITARY CONFLICTS AFTER THE SECOND WORLD WAR

The battle actions during the Second World War, characterised by large scale, fast rhythms and frequent changes of situation, imposed the tank on the battlefield by combining the following characteristics: execution of a strong fire, power of penetration, mobility, possibility to achieve surprise and influence the morale of the opponent.

The enhancement of these characteristics of the tanks was made possible by the aviation support and the mechanisation of all the weapons of the ground forces that constituted the German armoured division, the artillery, the infantry and the logistic support vehicles.

The interest shown in the continuous increase of firepower, mobility and ballistic protection led to remarkable achievements of tanks, which have been in a permanent process of improvement ever since.

The development and improvement of tanks after the Second World War were carried out in two basic directions:

- creation of new types;
- modernisation of existing models in equipment and manufacturing.

We believe that the first direction ensures a significant increase in the fighting qualities and the efficiency of the tanks, but the resources used are really high. The second direction is, in fact, the continuous process of introducing technological and constructive innovations in order to increase the fighting qualities and the duration of service. It is appreciated that this path enables the rapid and cost-effective achievement of tanks efficiency and a certain level of performance required in accordance with the increasing demands of the modern battlefield.

Between 1950 and 1955, due to the emergence of the nuclear weapon, it was believed that the tanks would lose the predominant role within the ground forces, considering that the carrier vectors of the new weapon (aviation and missiles) represented the main concern of the arms manufacturers. This idea was reconsidered, the tanks proving to be the most suitable fighting technique for exploiting the effects of the nuclear weapon. As a result, intensive research was carried out to adapt the tanks to the specific requirements of conducting combat actions under the new conditions, with a focus on the protection against the effects of nuclear explosions.

The local wars that took place after the Second World War represented real grounds for experimenting with new models of weaponry and fighting technique, ammunition and equipment, the results obtained being taken into consideration in the scientific research on the development of some models and types of weaponry more refined, more destructive.

The third Arab-Israeli war, the Yom Kippur War, which lasted from 6 to 26 October 1973, began with the surprise and simultaneous attack of Egypt and Syria against

Israel, on the Day of Atonement, the most important Jewish fasting day. It was known as the *"war of tactical guided missiles"*[28], being particularly different from previous local wars. During the combat actions, the latest weapons systems were used, with the use of large-scale guided missiles (different anti-tank missiles, anti-aircraft and aviation missiles). Many tanks (produced in Russia) were used by Syria on the Golan Heights and by Egypt on the Sinai Peninsula against the Israeli tanks (produced in the US and UK). The sudden increase in the efficiency of conventional means of fighting tanks led to the conclusion that the main characteristics of the tanks needed to be continuously enhanced: firepower, mobility and protection.

During the Yom Kippur War, it was found that tanks that were penetrated by an anti-tank missile, such as the Saggers used by the Egyptians, were burning because the hydraulic turret drive fluids were flammable. The solution was to mount the electric engines.

The war in Afghanistan, which started in 1979 and lasted for over a decade, led to a real armament test between Afghan forces (supported by Russia) and the mujahideen Islamist rebels (supported by the US, Saudi Arabia, Iran and Pakistan). The fact that Moscow no longer supplied weapons for the Najibullah regime at the end of 1991 and the mujahedin took over the control of the capital in April 1992 did not mean the end of the fighting. In this conflict, various shields were tested, including the additional shields added to the modernised Phase II T-55 tank[29], (see *figure no. 3*).

Figure no. 3: The modernised Phase II T-55 tank[30]

The Gulf War (Operation *"Desert Storm"*, in 1991), considered to be the largest post-war military confrontation, faced very large quantities of the newest categories of technology. The forces of the US-led international coalition showed that, instead of relying on different types of weapons, their current armed forces

[28] Toma Pleșanu, *Organizarea generală a blindatelor*, Editura Academiei Tehnice Militare, București, 1998, p. 28.
[29] *Ibid*, p. 29.
[30] Source: MFA Mizil.

relied on complex systems of families of weapons integrated by electronic means of communication and control.

The Iraq War (2003) was an example of joint combat actions, the land, naval and air forces being used remarkably and much more united (interoperable) than they were in 1991, in the Gulf War. Analysts believe that an important factor in winning the war was the firepower of allied forces: cruise missiles and heavy bombers hit targets with extraordinary accuracy; Abrams M1A1 tanks *(figure no. 4)*

Figure no. 4: M1A1 Abrams tank[31]

or Challenger 2 *(figure no. 5)* destroyed the Iraqi tanks T-55, or T-72 *(figure no. 6)*, obsolete and outdated, by firing directly from a distance of two miles; Apache attack helicopters provided air support, which meant that there was no equal competition from the beginning.

Figure no. 5: Challenger 2 tank[32]

This was the first war in history in which precision weapons were used with such a lethal effect, with intelligent ammunition being used at 70 percent, compared to only 7 percent in 1991.

[31] http://www.primeportal.net/tanks/m1_abrams.htm.
[32] http://www.armedforces.co.uk/army/listings/army4b7.htm.

Figure no. 6: T-72 tank[33]

The war in Iraq finally changed the perception that the tank was surpassed by the evolution of the battlefield and could no longer be used in military action. The effectiveness of the 65 tons Abrams and the 75 tons Challenger battle tanks questioned the statement that a light armoured vehicle over 20 tons (even equipped with large-calibre cannon, for example, 105 mm L1) is a real alternative to the heavy armoured tank.

During the *Cold War*, tanks were developed predominantly to fight in the open plains of northwestern Europe. The NATO and Warsaw Pact forces had pre-positioned field formations ready to be placed to counter any threat. One factor that affected the operating environment was the transit of the population from rural to urban areas. The fact that tanks had many vulnerabilities when it came to being used in urban areas made them unusable in military actions in the urban environment.

Tanks and armoured fight vehicles have played a significant role in the military operations of the past 18 years (2001 War in Afghanistan, 2003 invasion of Iraq, 2006 War in Lebanon between Israel and Hezbollah paramilitary groups, 2008 conflict between Russia and Georgia, 2013 French intervention in Mali and wars in eastern Ukraine and Syria). As a result of these operations, there was a need to increase the personnel protection, the installation of new electronic components as well as the remote-controlled armament, which implicitly led to an increase in weight.

CONCLUSIONS

From the beginning, tanks have revolutionised the art of war because they have led to increased mobility and protection of the forces involved in the conflict, and offered greater offensive and destructive power.

[33] Source: https://ro.pinterest.com/pin/466474473881834853/.

Initially, the theory regarding the tactics of using tanks in military conflicts was based on the harmonisation of their combat power with the existing combat methods, infantry tactics and the artillery. The tanks were involved in many military conflicts, contributing to the implementation of new operational concepts.

The lethal tank-aircraft combination was used by the Germans in the Second World War for the East and West campaigns. After the heyday of the Second World War, due to technological advances, tanks have continued to develop and play a decisive role on the battlefield. Requiring fire, air and ground support as well as high logistics, armoured vehicles have been designed and developed for tank support, which has led to the establishment of mechanised structures.

Analysing the latest achievements and developments in the field of armoured vehicles, many military experts are confident that the tanks will continue to be present on the battlefields including for the celebration, in 2116, of two centuries since their appearance[34]. It remains to be seen what they will look like in a century from now.

BIBLIOGRAPHY

1. Asociația culturală *"Valeriu Florin Dobrinescu", Armata română și evoluția armei tancuri. Documente (1919-1945)*, Editura Universității de Stat din Pitești, Pitești, 2012.
2. K.H. Frieser, *Mitul Blitzkrieg-ului, Campania din Vest a Wehrmacht-ului 1940*, Editura Militară, București, 2010.
3. Toma Pleşanu, *Organizarea generală a blindatelor*, Editura Academiei Tehnice Militare, București, 1998.
4. Spencer C. Tucker, *Weapons and Warfare Series, Tanks, An Illustrated History of their Impact,* ABC-CLIO, Inc., 2004.
5. http://www.primeportal.net/tanks/m1_abrams.htm.
6. https://ro.pinterest.com/pin/466474473881834853/.
7. http://www.armedforces.co.uk/army/listings/army4b7.htm.
8. https://www.historia.ro/sectiune/general/articol/un-mit-al-propagandei-sovietice-kursk-1943-cea-mai-mare-batalie-de-tancuri-din-istorie.
9. http://www.encyclopedia.com/social-sciences-and-law/political-science-and-government/ military-affairs-nonnaval/military-tank.
10. http://www.chars-francais.net/2015/index.php/engins-blindes/chars?task=view&id=688.
11. http://www.globalsecurity.org/military/systems/ground/tank-history1.htm.
12. http://www.army-technology.com/features/featuretimeline-100-years-of-tanks-5694455/.
13. https://www.cfc.forces.gc.ca/259/290/289/286/lamontagne.pdf.
14. https://www.the-blueprints.com/blueprints/tanks/tanks-r/72310/view/renault_ft-17_8mm_1917/.
15. https://www.globalsecurity.org/military/systems/ground/tank-history1.htm.
16. http://www.army-technology.com/features/featurewhat-does-the-future-hold-for-tanks-5688047/.

[34] http://www.army-technology.com/features/featurewhat-does-the-future-hold-for-tanks-5688047/.

THE USE OF KNOWLEDGE BANK TECHNOLOGIES AND SERVICES PROVIDED FOR THE FIELD OF DEFENSE, PUBLIC ORDER AND NATIONAL SECURITY

Radu Mihai OANȚĂ
PhD Candidate, "Carol I" National Defence University, Bucharest

Gheorghe MARCU
PhD Candidate, "Carol I" National Defence University, Bucharest

Toma PLEŞANU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Marinel-Adi MUSTAȚĂ, PhD
Associate Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

The knowledge-based society, in which knowledge is more and more accessible due to the rapid advancement of the IT, needs quick solutions for documentation. Taking into account the progressive development of the documentation needs in different fields, both at the organisational and individual level, we have thought of presenting several issues concerning the use of technologies and services provided by a knowledge bank for defence, public order and national security field.

In this paper, we will make a short introduction of the above-mentioned knowledge bank, followed by brief research of a pilot study in which we have meant to analyse the way its usefulness is perceived. Having this in mind, we have researched the perception of the technologies and services offered by it, by means of an online questionnaire, which actually served as a way to establish the level of being acquainted with the technology of the mentioned field. We should also mention the fact that the presented research study is meant to make users aware of the knowledge in the sector of knowledge banks with predominant applicability in the design and establishment of the knowledge bank for defence, public order and national security field. Moreover, the research is meant to deliver conclusions that will possibly enhance efficiency in developing some similar knowledge banks.

Keywords: knowledge bank, databases, services, sections, sorting.

INTRODUCTION

The knowledge bank for the field of defence, public order and national security is, in fact, a database containing knowledge. It aims to collect knowledge from the scientific and non-academic environment, promoting, disseminating and storing them through a descriptive and administrative coding scheme with *"Metadata Encoding and Transmission Standard"* (METS) transmission standards. The METS standard provides structured metadata in a digital library, so that access and knowledge transfer are very fast.

The digitised knowledge will be identified unequivocally, directly from the browser of a web user. The end-user can directly quote an individual resource, not needing to mention the website of an entire project.

The types of materials that will be included in the Knowledge Bank will be the following: bachelor's, dissertations, doctoral theses, scientific papers published in the volumes of national and international conferences, specialised publications, scientific research reports, course supports, both in electronic format obtained after scanning hard-copy documents, as well as in soft-copy format, current library resources and multimedia materials.

The basic concept based on which the knowledge bank will work is user orientation, focus on user requirements, identifying their needs and desires, meeting their timely needs, providing the expected qualities and quantities in an efficient and operative way[1].

Possible operations that can be performed by the user of the knowledge bank for the domain AOPSN are shown in *figure no. 1*.

STUDY ON THE LEVEL OF KNOWLEDGE OF THE TECHNOLOGIES AND SERVICES OFFERED BY THE KNOWLEDGE BANK FOR THE FIELD OF DEFENSE, PUBLIC ORDER AND NATIONAL SECURITY

We will briefly present some aspects of the research of a pilot study in which we tried to determine how the use of the knowledge bank for the field of defence, public order and national security (AOPSN) is perceived. An investigation of the perception of multimedia technologies and services was carried out using an online

1 R.M. Oanță, T. Pleșanu, *Knowledge Sharing – The First Step towards Building up a Knowledge Bank*, the 14th International Scientific Conference *"Strategies XXI"*, Strategic Changes in Security and International Relations, București, 2018, pp. 213-219.

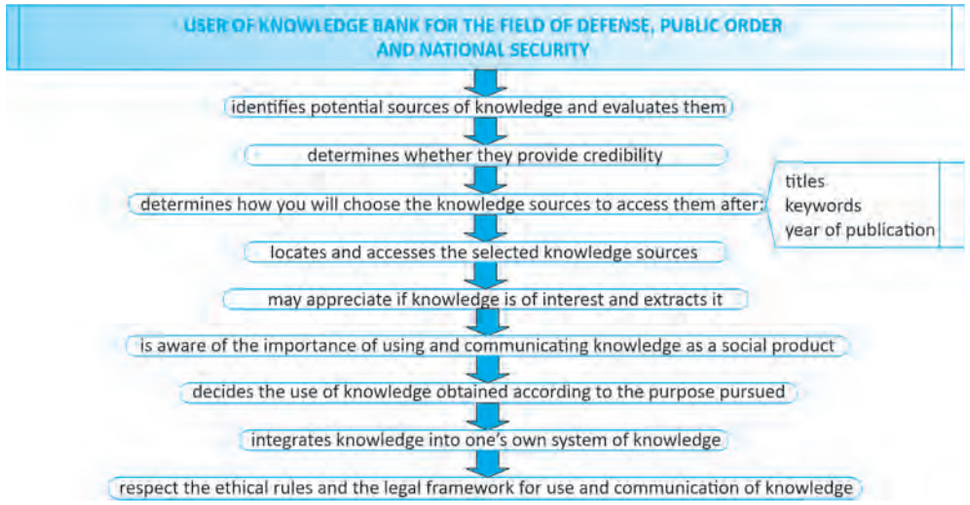


Figure no. 1: Operations carried out by a knowledge bank user for the field of AOPSN

questionnaire. This also allowed determining the level of knowledge in the field, as well as establishing the degree of appreciation on the field.

The research

The research is based on the considerations that characterise the knowledge banks and guarantees the efficiency of the development of these platforms at the national level.

The instrument used in the research allowed determinations of the quantitative and qualitative nature of the elements related to different banks of knowledge.

The questionnaire, comprising a total of 27 questions per section, was designed with the help of Google Forms, a component of the Google Drive application (Disk with Documents) that allows surveys or the creation of lists with a simple online form and consultation of results well organised in a spreadsheet or summary for this research and determines the opinions, arguments and level of knowledge of the technologies and services provided by the knowledge bank of AOPSN.

The research objectives were developed in a concrete and measurable way, eliminating vague expressions both in designing and adapting questions and in formulating research conclusions and results. The objectives proposed for this research are:

- providing empirical benchmarks regarding the market profile of interested organisations;
- identifying the level of familiarisation of the questioned personnel with the elements provided by the knowledge banks;

- determining the level of appreciation of the different services offered by the knowledge bank for the domain AOPSN;
- identifying how the questioned personnel value the classic technologies compared to the modern ones;
- drawing conclusions necessary to open research directions.

The testing was performed online, and in the creation of the questionnaire it was taken into account the alternation of open and closed questions, a fact imposed by the research objectives and methodological criteria for making it increasingly appealing.

The process of creating the questionnaire took place within a focus group, where the answers to a set of questions addressed to decision-makers from several structures of the Ministry of Interior were taken into account. The question was whether they knew the different applications of the sites of the Web 2.0[2] platform, elements used in the realisation of the knowledge bank and whether they used or found it beneficial to use the concept of lessons learned. The concept of the interview was posted on the Google Drive application storage and corresponds to the email address *lectii.invatateMAI@gmail.com*[3]. The application of the interview guide in an extended format is also uploaded to the storage mentioned above[4]. The content of the interviews is very varied, touching on all aspects of the state of knowledge in the field of organisational learning[5].

There was an expert checking of the questions, namely an electronic engineer, currently being employed within the information technology branch, with profile studies in the field of communications and information technology, and having about 20 years of experience in the field, as well as teachers with specialisations in the fields of science, economics and humanities, from the organising structure of the doctoral studies program in the field of military sciences, within the *"Carol I"* National Defence University.

The questionnaire was pretested on a pool of 30 subjects, of various genders, ages, studies and from different dimensions of the defence, public order and national security system. Following the pretesting, some formulations that made various items ambiguous were modified.

---

2 R.M. Oanță, *Ways of Using the Web 2.0 Service Models within the NSDPONS*, the 15th International Scientific Conference *"Strategies XXI"*, Strategic Changes in Security and International Relations, București, 2019, pp. 212-221.

3 https://drive.google.com/drive/folders/1TyB3tvNtJTQOqL5_J3bL5POtqq1bYRUI?usp=sharing

4 https://drive.google.com/drive/folders/1R7boiwEveKF1Z32YyNEcW_d4ZzIaO7tM?usp=sharing

5 R.M. Oanță, *Procesul implementării lecțiilor învățate la nivelul Ministerului Afacerilor Interne*, Buletinul Universității Naționale de Apărare *"Carol I"*, no. 2, București, 2019, pp. 56-62.

The questionnaire was taken by a total of 109 subjects, with the same jobs as the subjects with whom the questionnaire was pretested, taking about 15 minutes to go through it.

The complete form of the questionnaire can be viewed on the GoogleDrive account *bancadecunostinte@gmail.com*, using the password: *banca.de.cunostinte*[6].

After receiving the answers from a number of 109 samples, the resulting data were exported centrally, drawing up spreadsheets in the Microsoft Excel program, belonging to the Microsoft Office suite, interpreted, processed and statistically analysed in the software *"Statistical Package"* for the Social Science (SPSS).

Data analysis, statistical processing and interpretation of results

The data analysis, the statistical processing and the interpretation of the results were done by testing some relevant statistical hypotheses in accordance with the tutorials presented by Adrian Vicențiu Lăbar in the work *"SPSS for Education Sciences"*[7].

To determine if those who want the knowledge bank to have lessons learned and good practices find it very important to use it so as to improve the level of preparation, we applied the t-test for independent samples. According to the answers sent to *question 17* of the questionnaire[8], there are significant differences regarding the importance of using the knowledge bank to improve the level of preparation by those who want it to contain lessons learned and good practices and those who do not. According to the Levene test (F = 4.429, p = 0.038), the variances of those who want the knowledge bank to contain lessons learned

[6] https://docs.google.com/forms/d/e/1FAIpQLSdJ9afVLRiGyCZWVQysP8LI-OVqwiC8JRa4DGaOZXNUe69d1g/viewform

[7] Adrian Vicențiu Labăr, *SPSS pentru științele educației*, București, Editura Polirom, 2008, pp. 87-117.

[8] https://docs.google.com/forms/d/e/1FAIpQLSdJ9afVLRiGyCZWVQysP8LI-OVqwiC8JRa4DGaOZXNUe69d1g/viewform.

and good practices and those who do not want are different. The chance of making a mistake is only 3.8% if we reject the null hypothesis.

t (108) = 2.691, p = 0.01.

Those who want the knowledge bank to have lessons learned and good practices consider important its usefulness to improve the level of preparation (M1 = 4.43) compared to those who do not want this (M2 = 4).

According to Cohen's criteria (1988), those who want the knowledge bank to have lessons learned and good practices find it very important to use it to improve the level of preparation for those who do not want it, r = 0.25. This implies that about 6% (r^2 = 0.06) of the variance of those who want the knowledge bank to have lessons learned and good practices is explained by the variance of the independent variable, respectively by their choice. The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1%.

To determine if those who want the knowledge bank to have lessons learned are familiar with the databases, we applied the t-test for independent samples. According to the answers sent to question number 1 of the questionnaire, there are significant differences regarding the familiarity of the respondents with the databases that want the knowledge bank to contain lessons learned and good practices and those who do not. According to the Levene test (F = 0.324, p = 0.466), the variances of those who want the knowledge bank to have lessons learned and good practices and those who do not want are equal. The chance of making a mistake is only 46.6% if we reject the null hypothesis.

t (108) = 2.426, p = 0.017.

Those who want the knowledge bank to have lessons learned and good practices are familiar with the databases (M1 = 4.30) compared to those who do not want (M2 = 3.86).

According to Cohen's criteria (1988), those who want the knowledge bank to contain lessons learned and good practices are familiar with databases versus those who do not want this, r = 0.23. This assumes that about 5% (r^2 = 0.05) of the variance of those who want the knowledge bank to have lessons learned and good practices is explained by the variance of the independent variable, respectively by their choice. The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1.7%.

We applied **Chi-square** tests in order to find a statistically significant association between the following variables:

Those who want the knowledge bank in the field of defence, public order and national security to have specialised publications and those who want to search the knowledge bank, the relevant knowledge according to the author.

$x^2(1) = 10.267$, p = 0.001. The effect size indicator Phi = 0.306, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

All the subjects who want the knowledge bank in the field of defence, public order and national security to contain specialised publications are interested in seeking the relevant knowledge in this bank by the author.

Those who want the knowledge bank in the field of defence, public order and national security to have specialised publications and those who want to search the knowledge bank, the relevant knowledge by topic.

$x^2(1) = 12.135$, p <0.001. The effect size indicator Phi = 0.332, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

All subjects who want the knowledge bank in the field of defence, public order and national security to contain specialised publications are interested in searching for the relevant knowledge in this bank by topic.

Those who want the knowledge bank in the field of defence, public order and national security to contain multimedia materials and those who want to search the knowledge bank, the relevant knowledge by topic.

$x^2(1) = 13.782$, p <0.001. The effect size indicator Phi = 0.354, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

All subjects who want the knowledge bank in the field of defence, public order and national security to contain multimedia materials are interested in searching for relevant knowledge in this bank by topic.

The way in which to contact the knowledge bank administrator (live chat window) and the position held by the respondents.

$x^2(1) = 10.559$, p = 0.001. The effect size indicator Phi = 0.311, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects holding an execution position want to contact the knowledge bank administrator through a live chat window.

How to contact the knowledge bank administrator (e-mail) and the role held by the respondents

$x^2(1) = 10.067$, p = 0.002. The indicator for evaluating the effect size Phi = - 0.304, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 2‰.

Subjects holding a management position want to contact the knowledge bank administrator by e-mail.

Search for knowledge in a knowledge base by title and contact the administrator of the knowledge bank platform by e-mail.

$x^2(2) = 16.285$, p <0.001. The effect size indicator Phi = 0.385, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects wishing to contact the knowledge bank administrator via email are interested in how to search for knowledge in a knowledge base by title.

Search for knowledge in a knowledge base by title and telephone contact of the administrator of the knowledge bank platform.

$x^2(2) = 15.178$, p = 0.001. The effect size indicator Phi = 0.371, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects wishing to contact the knowledge bank administrator by telephone are interested in how to search for knowledge in a knowledge base by title.

Search for knowledge in a knowledge base by title and view the most accessed works by the sorting method after accessions.

$x^2(2) = 22.231$, p <0.001. The effect size indicator Phi = 0.450, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects who want to view the most accessed works by the sorting method after accessions are interested in how to search for knowledge in a knowledge base by title.

Those who want to search for certain knowledge in a knowledge base by author and those who consider the most relevant section for the knowledge bank the recently added section.

$x^2(1) = 19.808$, p <0.001. The effect size indicator Phi = 0.424, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects who wish to search for certain knowledge in a knowledge base by author consider the most relevant section for the knowledge bank the recently added section.

Those who wish to seek certain knowledge in a knowledge base by author and those who consider the section most relevant to the knowledge bank the terms and conditions section.

$x^2(1) = 23.042$, p <0.001. The effect size indicator Phi = 0.458, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects wishing to seek certain knowledge in a knowledge base by author consider the most relevant section for the knowledge bank the terms and conditions section.

Those who want to search for certain knowledge in a knowledge base by author and contact method of knowledge bank administrator by email.

$x^2(1) = 11{,}698$, $p = 0.001$. The effect size indicator Phi = 0.326, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Subjects who wish to search for certain knowledge in a knowledge base after the author wishes to contact the knowledge bank administrator by e-mail.

Those who want to seek certain knowledge in a knowledge base by author and the size of their field of activity.

$x^2(2) = 13.349$, $p = 0.001$. The effect size indicator Phi = 0.355, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Respondents within the public order dimension want to seek certain knowledge in a knowledge base by author.

There is an association between the size of the domain of activity respondents and the contact method of the knowledge bank administrator by e-mail.

$x^2(2) = 13.076$, $p = 0.001$. The effect size indicator Phi = 0.351, the effect size is moderate. The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is 1‰.

Respondents within the defence dimension want to contact the knowledge bank administrator via email.

There is a positive **Spearman** correlation between familiarising respondents with databases and assessing the usefulness of the knowledge banks used.

$\rho(59) = 0.334$, $p = 0.008$.

As the correlation coefficient ρ is an expression of the magnitude of the effect, referring to Cohen's (1988) criteria, it turns out that the relation between the respondents' familiarity with the databases and the assessment of the usefulness of the knowledge banks used is average. So, the effect size is average. The hypothesis is verified and the chance to fail by rejecting the null hypothesis is 8‰.

The more you are familiar with databases, the more satisfied you are with the usefulness of knowledge banks.

There is a positive correlation between the familiarity of the respondents with the databases and the importance of using the knowledge bank to improve the level of training.

$\rho(108) = 0.332$, $p < 0.001$, the effect size is average.

The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is less than 1‰.

The more you are familiar with databases, the more you are aware of the importance of using the knowledge bank to improve the level of preparation.

There is a positive correlation between assessing the usefulness of the knowledge banks used and the importance of the security of the data contained on the website hosting the knowledge bank.

$\rho(59) = 0.312$, $p = 0.014$, the effect size is average.

The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is less than 14‰.

Those who find it important to use the knowledge banks are interested in the security of the data contained on the website that hosts the knowledge bank.

There is a positive correlation between assessing the usefulness of the knowledge banks used and the importance of using the knowledge bank to improve the level of training.

$\rho(59) = 0.259$, $p = 0.043$, the effect size is weak.

The probability of producing the type I error, respectively, of rejecting the null hypothesis when it should have been accepted is less than 43‰.

Those who find it important to use knowledge banks find it necessary to use the knowledge bank to improve their level of training.

There is a positive correlation between those interested in sharing knowledge through the knowledge bank and those interested in sharing knowledge through the knowledge bank.

$\rho(106) = 0.788$, $p < 0.001$, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1 ‰.

Those interested in sharing knowledge through the knowledge bank are also interested in the exchange of knowledge through the knowledge bank.

There is a positive correlation between those interested in sharing knowledge through the knowledge bank and those interested in knowledge deposits.

$\rho(106) = 0.900$, $p < 0.001$, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in sharing knowledge through the knowledge bank are also interested in knowledge deposits.

There is a positive correlation between those interested in sharing knowledge through the knowledge bank and those interested in knowledge transfer.

ρ (105) = 0.824, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in sharing knowledge through the knowledge bank are also interested in knowledge transfer.

There is a positive correlation between those interested in sharing knowledge through the knowledge bank and those interested in reusing knowledge.

ρ (104) = 0.837, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in sharing knowledge through the knowledge bank are also interested in reusing knowledge.

There is a positive correlation between those interested in sharing knowledge through the knowledge bank and those interested in the interface of the website that hosts the knowledge bank.

ρ (107) = 0.292, p = 0.002, the effect size is weak.

The hypothesis is verified and the chance to fail by rejecting the null hypothesis is 2‰.

Those interested in sharing knowledge through the knowledge bank are also interested in the interface of the website that hosts the knowledge bank.

There is a positive correlation between those interested in knowledge exchange through the knowledge bank and those interested in knowledge deposits.

ρ (106) = 0.783, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1 ‰.

Those interested in the exchange of knowledge through the knowledge bank are also interested in knowledge deposits.

There is a positive correlation between those interested in knowledge exchange through the knowledge bank and those interested in knowledge transfer.

ρ (105) = 0.888, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1 ‰.

Those interested in the exchange of knowledge through the knowledge bank are also interested in the transfer of knowledge.

There is a positive correlation between those interested in the exchange of knowledge through the knowledge bank and those interested in the reuse of knowledge.

ρ (104) = 0.796, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in the exchange of knowledge through the knowledge bank are also interested in the reuse of knowledge.

There is a positive correlation between those interested in the exchange of knowledge through the knowledge bank and the importance of using the knowledge bank to improve the level of preparation.

ρ (106) = 0.224, p = 0.002, the effect size is weak.

The hypothesis is verified and the chance to fail by rejecting the null hypothesis is 2‰.

Those interested in the exchange of knowledge through the knowledge bank find it important to use the knowledge bank to improve the level of training.

There is a negative correlation between those interested in the exchange of knowledge through the knowledge bank and the most advanced form of graduate training.

ρ (106) = -0.204, p = 0.034, the effect size is weak.

The hypothesis is verified and the chance to fail by rejecting the null hypothesis is 34 ‰.

Those interested in the exchange of knowledge through the knowledge bank are not the ones who have graduated with the highest form of training. The more learned the respondents are, the more they are disinterested in the exchange of knowledge through the knowledge bank.

There is a positive correlation between those interested in knowledge deposits through the knowledge bank and those interested in knowledge transfer.

ρ (105) = 0.798, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in knowledge deposits through the knowledge bank are also interested in knowledge transfer

There is a positive correlation between those interested in knowledge deposits through the knowledge bank and those interested in reusing knowledge.

ρ (104) = 0.793, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in knowledge deposits through the knowledge bank are also interested in the reuse of knowledge.

There is a positive correlation between those interested in knowledge deposits through the knowledge bank and those interested in the interface of the website hosting the knowledge bank.

ρ (106) = 0.230, p = 0.017, the effect size is weak.

The hypothesis is verified and the chance to fail by rejecting the null hypothesis is 17‰.

Those interested in knowledge deposits through the knowledge bank are also interested in the interface of the website that hosts the knowledge bank.

There is a positive correlation between those interested in the transfer of knowledge through the knowledge bank and those interested in the reuse of knowledge.

ρ (103) = 0.833, p <0.001, the effect size is very strong.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1‰.

Those interested in the transfer of knowledge through the knowledge bank are also interested in the reuse of knowledge.

There is a positive correlation between those interested in the transfer of knowledge through the knowledge bank and those interested in the interface of the website hosting the knowledge bank.

ρ (106) = 0.275, p = 0.004, the effect size is weak.

The hypothesis is checked and the chance of failing by rejecting the null hypothesis is 4‰.

Those interested in the transfer of knowledge through the knowledge bank are also interested in the interface of the website that hosts the knowledge bank. There is a positive correlation between those interested in the reuse of knowledge through the knowledge bank and those interested in the interface of the website hosting the knowledge bank. ρ (106) = 0.239, p = 0.014, the effect size is weak. The hypothesis is verified and the chance to fail by rejecting the null hypothesis is 14 ‰.

Those interested in the reuse of knowledge through the knowledge bank are also interested in the interface of the website that hosts the knowledge bank.

There is a positive correlation between those interested in the security of the data contained on the website that hosts the knowledge bank and the importance of using the knowledge bank to improve the level of preparation.

ρ (108) = 0.464, p <0.001, the effect size is average.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 1 ‰. Those interested in the security of the data contained on the website that hosts the knowledge bank are also interested in the use of the knowledge bank to improve the level of training.

There is a negative correlation between those interested in the security of the data contained on the website that hosts the knowledge bank and the frequency of using the knowledge bank.

ρ (107) = -0.276, p = 0.004, the effect size is weak.

The hypothesis is checked and the chance of failing by rejecting the null hypothesis is 4‰.

Those interested in the security of the data contained on the website that hosts the knowledge bank do not access the knowledge bank very often.

There is a negative correlation between those interested in the interface of the website hosting the knowledge bank and the age of the respondents.

ρ (106) = -0.249, p = 0.009, the effect size is weak.

The hypothesis is verified and the chance of failing by rejecting the null hypothesis is 9‰.

As the respondents are older, they are not interested in the interface of the website hosting the knowledge bank and the age of the respondents.

There is a negative correlation between those interested in the interface of the website hosting the knowledge bank and the form of completed training.

ρ (108) = -0.270, p = 0.004, the effect size is weak.

The hypothesis is checked and the chance of failing by rejecting the null hypothesis is 4‰.

It does not matter the most advanced form of graduate training when choosing the interface of the website that hosts the knowledge bank.

CONCLUSIONS

Following a careful study of knowledge banks worldwide and interpreting the results of the research, as for conclusions, we thought it would be more useful to outline some considerations that could be the basis for the implementation of useful strategies, in order to achieve the knowledge bank for the field of defence, public order and national security:

- those who want the knowledge bank to have lessons learned and good practices find it very important to use it to improve the level of preparation;
- those who are familiar with the databases want the knowledge bank to have lessons learned and good practices;
- all the subjects who want the knowledge bank to contain specialised publications are interested in seeking relevant knowledge in this bank by author and by subject;
- individuals filling an execution position want to contact the knowledge bank administrator through a live chat window;

- the subjects that occupy a management position want to contact the manager of the knowledge bank by e-mail;
- the subjects who want to see the most accessed works by the sorting method after the accessions are interested in the search of knowledge in a knowledge base by title;
- the subjects who wish to search for certain knowledge in a knowledge base after the author considers the most relevant section for the knowledge bank the recently added section;
- respondents in the public order dimension want to seek certain knowledge in a knowledge base by the author;
- the respondents within the defence dimension want to contact the knowledge bank administrator by e-mail;
- the more you are familiar with databases, the more you are aware of the importance of using the knowledge bank to improve the level of preparation;
- those who find it important to use the knowledge banks are interested in the security of the data contained on the website that hosts the knowledge bank;
- those interested in sharing knowledge through the knowledge bank are also interested in the exchange, deposits, transfer of knowledge and reuse of knowledge through the knowledge bank. at the same time respondents interested in one of the services provided by the knowledge bank (sharing, exchange, deposit, transfer and reuse) are also interested in the others;
- those interested in the exchange of knowledge through the knowledge bank find it important to use the knowledge bank to improve the level of preparation;
- the more educated the respondents, the more they are disinterested in the exchange of knowledge through the knowledge bank;
- respondents interested in the services provided by the knowledge bank (sharing, exchange, deposit, transfer and reuse) are also interested in the interface of the website that hosts the knowledge bank;
- those interested in the security of the data contained on the website that hosts the knowledge bank are also interested in the importance of using the knowledge bank to improve the level of training.

The main barriers and limits that made it difficult to achieve the objectives are the following:

1. the statistical power is relatively small because in the research we had a small sample, in this sense, the study can be considered a pilot;

2. the research was based in particular on the statements of the respondents, who may unconsciously or deliberately distort the information that describes the reality;
3. the ability of the questioned subjects to objectively assess the researched elements and the memory errors that are directly proportional to the time elapsed since the events that are the subject of our research;
4. the sampling technique used, the *"snowball technique"*, does not allow extrapolation of the study results;
5. bibliographic sources related to the researched domain are limited.

BIBLIOGRAPHY

1. Adrian Vicențiu Labăr, *"SPSS pentru științele educației"*, Editura Polirom, București, 2008;
2. R.M. Oanță, *Ways of Using the Web 2.0 Service Models within the NSDPONS*, the 15th International Scientific Conference *"Strategies XXI"*, *Strategic Changes in Security and International Relations*, București, 2019.
3. R.M. Oanță, T. Pleșanu, *Knowledge Sharing – The First Step towards Building up a Knowledge Bank*, the 14th International Scientific Conference *"Strategies XXI"*, *Strategic Changes in Security and International Relations*, București, 2018.
4. R.M. Oanță, *Procesul implementării lecțiilor învățate la nivelul Ministerului Afacerilor Interne*, Buletinul Universității Naționale de Apărare *"Carol I"*, no. 2, București, 2019.

THE INFLUENCE OF THE CHARACTERISTICS OF FUTURE CONFLICTS ON THE SHAPE OF TANK STRUCTURES IN THE ROMANIAN LAND FORCES

Nicolae PLEȘANU

PhD Candidate, "Carol I" National Defence University, București

Ghiță BÂRSAN, PhD

Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

Sorin-Gheorghe PÎNZARIU, PhD

Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

The process of reform of the Romanian Armed Forces, initiated after 1990, has had multiple consequences on the tank structures, by reducing their number. In this article, we will present the characteristics of future conflicts and how they will influence the shape of future tank structures of the Romanian Land Forces. We will show several versions of the reorganisation of tank structures that can be used in future conflicts.

Keywords: operational environment, future conflicts, reorganisation, structure, organisation.

INTRODUCTION

The future operational environment will be characterised by uncertainty. Military engagements in crises and intra-state conflicts will be more common but military engagement in a major interstate conflict is not excluded.

The armed forces are not the only element that can contribute to a safe and secure future operational environment. They must train not only for major fights but also for different types of activities on the future battlefield, at the same time and together with other military and non-military actors (international organisations, government and non-governmental organisations) with which they must be able to work.

CONSIDERATIONS ON THE CHARACTERISTICS OF FUTURE CONFLICTS

To predict the features of future conflicts, we will start from the characteristics of the future operational environment.

The operational environment or the action environment is defined as a *"system of systems in which each of the actors interacts with the others, pursuing its own interests. They develop strategies and allocate resources to carry out the actions necessary to achieve the power that enables them to exert influence on others and reach their own objectives"*[1].

In our opinion, future conflicts will be determined by complex combinations of historical, political, military, social, religious, cultural and economic factors. A useful tool for viewing and understanding the future operational environment as accurately as possible is the political, military, economic, social, informational and infrastructure analytical model (PMESII)[2].

At the same time, we consider that the future operating environment will be conditioned by the following factors:

- complexity and uncertainty;
- access to vital resources;
- the population as a centre of gravity (definition of the term is presented in glossary with terms and definitions);
- urbanisation;

[1] SMG-103, *Doctrina Armatei României*, București, 2012, p. 135.

[2] SMFT-10, *F.T.-1, Doctrina operațiilor forțelor terestre,* București, 2017, p. II-2.

- demographic growth;
- population migration.

The future operational environment will also be influenced by the presence of the following determining factors in obtaining the desired final state by belligerents:

- the human factor;
- technological factor.

These two factors are in a permanent interdependence relation that must be continuously optimised.

The environmental or ecological factor remains an element that will influence the physiognomy of conflicts in the future.

According to the *Doctrine of Land Forces Operations*, future conflicts, regardless of their typology, "*country's defence war, alliance war*" or "*coalition war*"[3], will be characterised mainly by:

- reduced military forces;
- greater concentration of forces in the decisive points;
- joint and priority multinational operations;
- rapid and discouraging reaction – including by performing preventive strokes;
- increased capacity for manoeuvre at all levels.

From the ones presented above and the analysis of the last wars and military conflicts, we can conclude that among the main features of the future conflicts could be the following:

- their deployment in all environments: land, sea, undersea, air, outer space, cyberspace information, psychological ones, in the media and economic areas;
- the use of diverse forces and means, with very high mobility, high firepower, precision and special target destruction and damage effects;
- use of lethal or non-lethal weapons, depending on the circumstances;
- huge consumption of ammunition, fuels and other resources to prepare, sustain and ensure the desired final state;
- huge material losses for the opponent;
- transparency of action environments due to the combined activity of observation and correction satellites, airborne radar and passive and active contact detection means;
- the use of high performing and very accurate weapons and weapon systems that enable effects on targets with minimal collateral damage;

[3] *Ibid*, p. I-2.

- the rapid concentrations and dispersions of forces and means;
- the tendency to avoid direct, frontal confrontations between numerous forces and means, focusing on actions with small but particularly effective formations by their firepower and with a special autonomy of action;
- the electronic saturation of the battlespace for the execution of strikes with its own means outside the opponent's response range;
- engaging in combat of real professionals, both in direct confrontation, man-to-man, and in cyberspace, psychic, economic and media;
- a pronounced international character (alliance or coalition);
- long-term traumatic psychological effects;
- low intervention duration.

The influence of these characteristics of future conflicts on the shape of tank structures in the Romanian Land Forces will be presented in the next chapter.

THE REORGANISATION OF TANK STRUCTURES IN THE ROMANIAN LAND FORCES

In our view, the characteristics of future conflicts as well as the reconfiguration of the components of the main battle tanks involve the reorganisation and transformation of current tank structures or the formation of new ones. We believe that future tank structures, within the Romanian land forces, as well as the concepts of combat, will have to be developed in such a way as to include new technological discoveries and ensure their strategic deployment when needed. These future structures, resulting from the reorganisation process, will be designed and trained to conduct military action in high-intensity conflicts, in complex terrain, but also in urban environments, in a joint context and against any type of potential enemy.

In this context, the future tank structures must be particularly mobile, have high reaction possibilities, as well as the ability to be deployed quickly and over long distances, over obstacles and in improper terrain, benefiting from the advantage of surprise and expanding the area of military operations in areas that cannot be immediately located by the opponent.

Starting from the current organisation of the combat structures within the Romanian Land Forces, here are two possible versions of organising the future tank structures, as follows:

- organisation by branch units;
- modular organisation, subunits of tanks and infantry.

Arrangement by weapon units

In our opinion, a possible version of tank structures organisation on branch units could be:

a. Version no. 1

- tank platoon (Tk. Pl.) organised in 4 tanks (Tk.) one of which is the platoon commander;
- tank company (Tk. Coy.) organised in 3 tank platoons (3 Tk. Pl. x 4 Tk. + 2 Tk. company command, total 14 tanks);
- tank battalion (Tk. Bn.) organised in 6 companies (Coy.) as follows:
  - combat subunits: 4 tank companies (4 Tk. Coy. x 14 Tk. + 2 Tk. battalion command, total 58 tanks);
  - support subunits: 1 combat support company (CS Coy.) and 1 Combat service support company (CSS Coy.);
- the combat support company has the following 5 structures of platoon level in the composition: reconnaissance, engineer, signal, CBRN defence and military police platoons;
- the combat service support company has the following 5 structures of the platoon level in the composition: medical, supply and transport, maintenance, logistical and food platoons.

This type of tank battalion by weapon units can be found in the mechanised brigades or within a tank brigade structure, a structure that does not exist at this time in the composition of the Romanian Army. The organisation of the tank battalion by weapon units, version no. 1, is shown in *figure no. 1*.

- tank brigade (Tk. Bde.) organised in the following structures:
  - combat structures: 3 tank battalions and 2 infantry battalions (Inf. Bn.), (3 Tk. Bn. x 58 Tk., a total of 174 tanks and 2 Inf. Bn. x 44 IFV[4], total 88 IFV);
  - tank battalion (Tk. Bn.) organised in 6 companies presented above;
  - infantry battalion organised on 3 infantry companies (Coy. Inf.), each company with 3 infantry platoons (Pl. Inf.) organised in 4 infantry fighting vehicle one of which is the platoon commander (3 Coy. Inf. x (3 Pl. Inf. x 4 IFV) + 3 x 2 IFV company command + 2 MLI battalion command, total 44 IFV));
  - support structures: 1 artillery battalion (Arty. Bn.), 1 antiaircraft defence battalion (AAD Bn.), 1 combat service support battalion (CSS Bn.);
  - brigade subunits: 1 reconnaissance company (Recce. Coy.), 1 engineer company (Engr. Coy.), 1 electronic warfare company (EW Coy.), 1 signal company (Sign. Coy.), 1 CBRN defence company (CBRN Def. Coy.) and 1 combat service support (CSS Coy.).

[4] Infantry fighting vehicle.

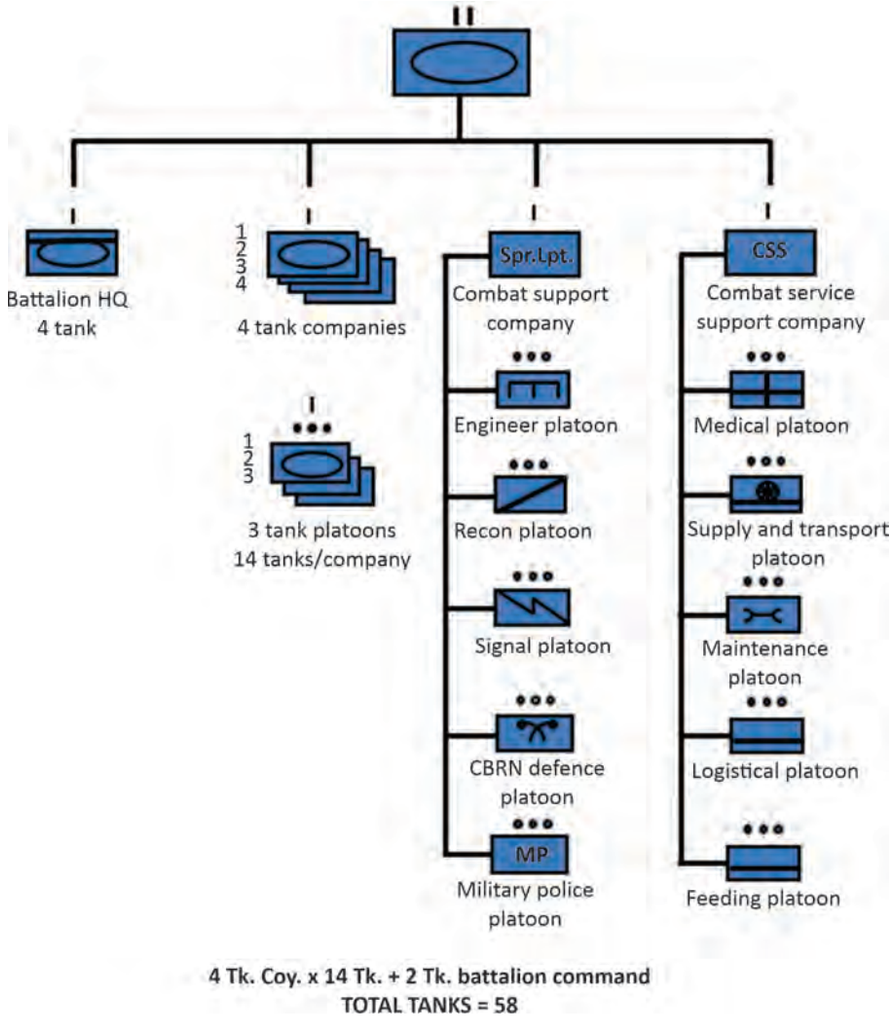


Figure no. 1: Organisation of the tank battalion by branch units, version no. 1.

The organisation of this type of tank brigade, by branch units, *version no. 1*, is shown in *figure no. 2.*

b. Version no. 2

- tank platoon (Tk. Pl.) organised in 5 tanks (Tk.) one of which is the platoon commander;
- tank company (Tk. Coy.) organised in 3 tank platoons (3 Tk. Pl. x 5 Tk. + 2 Tk. company command, total 17 tanks);

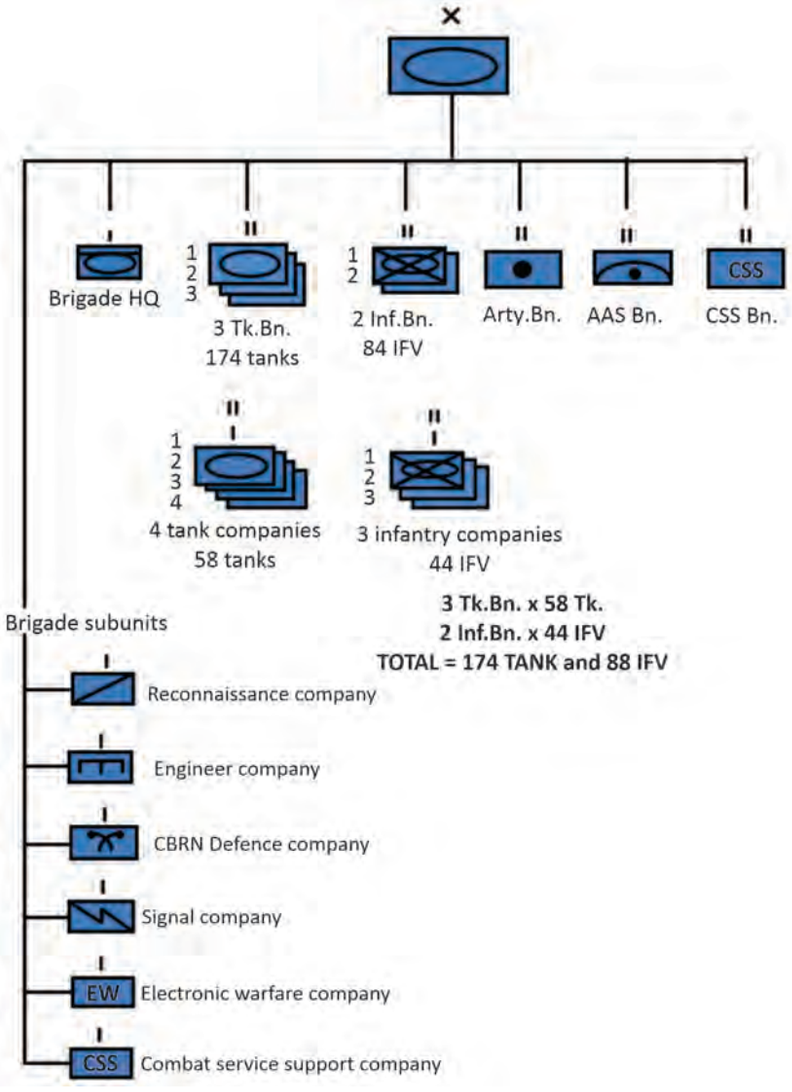


Figure no. 2: Organisation of the tank brigade by branch units, version no. 1.

- tank battalion (Tk. Bn.) organised in 5 companies (Coy.) as follows:
  - combat subunits: 3 tank companies (3 Tk. Coy. x 17 Tk. + 3 Tk. battalion command, total 54 tanks);
  - support subunits: 1 combat support company (CS Coy.) and 1 Combat service support company (CSS Coy.). The organisation of these two companies is like the one presented at the tank battalion by branch units, *version no. 1*.

This tank battalion-like structure on branch units can be found in mechanised brigades or within a tank brigade structure. The organisation of the tank battalion by branch units, version no. 2, is shown in *figure no. 3*.

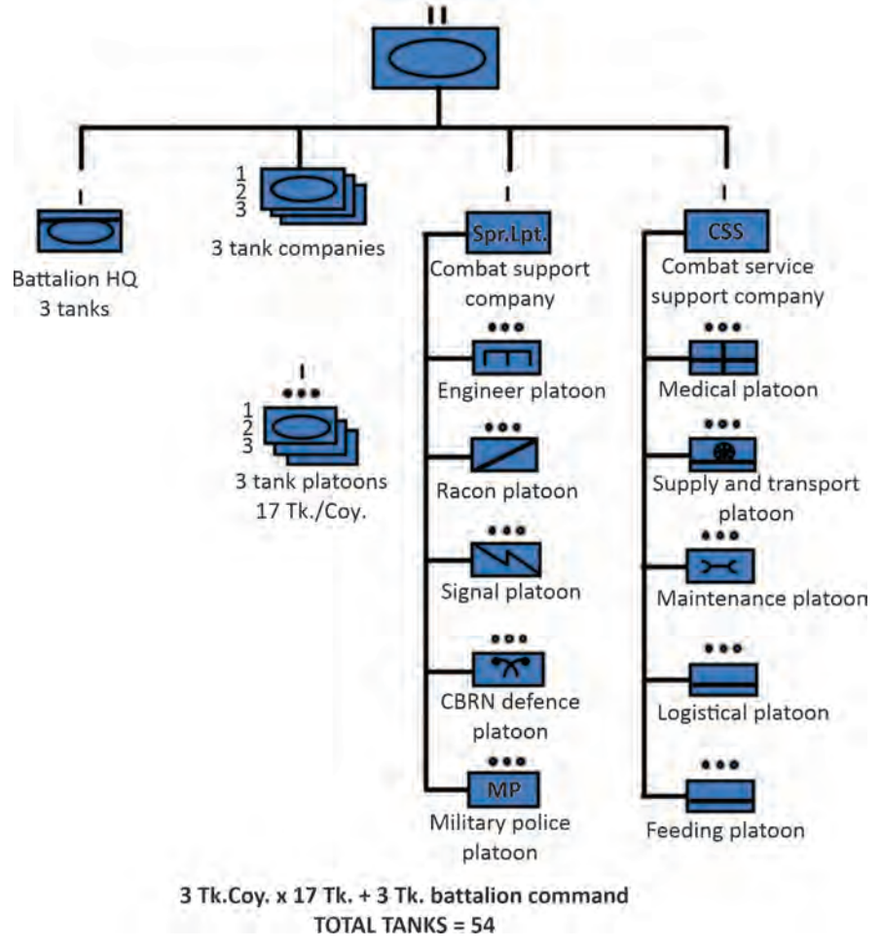


Figure no. 3: Organisation of the tank battalion by branch units, version no. 2.

- tank brigade (Tk. Bde.) organised in the following structures:
  - combat structures: 2 tank battalions (2 Tk. Bn. x 54 Tk., total 108 tanks) and 2 infantry battalions, (2 Inf. Bn. x 44 IFV, total 88 IFV);
  - support structures: 1 artillery battalion (Arty. Bn.), 1 antiaircraft defence battalion (AAD Bn.), 1 combat service support battalion (CSS Bn.);
  - brigade subunits: 1 reconnaissance company (Recce. Coy.), 1 engineer company (Engr. Coy.), 1 electronic warfare company (EW Coy.), 1 signal company (Sign. Coy.), 1 CBRN defence company (CBRN Def. Coy.) and 1 combat service support (CSS Coy.).

The organisation of the tank brigade by branch units, *version no. 2*, is shown in *figure no. 4.*

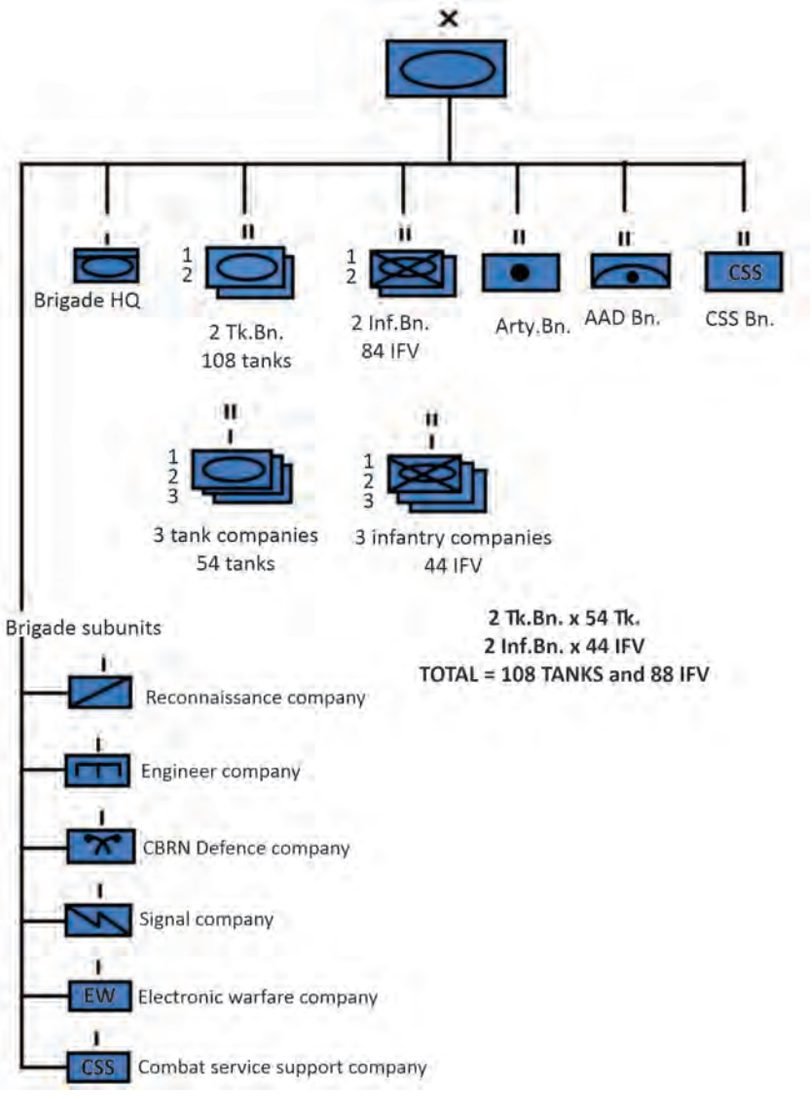


Figure no. 4: Organisation of the tank brigade by branch units, version no. 2.

c. Version no. 3

- tank platoon (Tk. Pl.) organised in 4 tanks (Tk.) one of which is the platoon commander;
- tank company (Tk. Coy.) organised in 3 tank platoons (3 Tk. Pl. x 4 Tk. + 2 Tk. company command, total 14 tanks);

- tank battalion (Tk. Bn.) organised in 5 companies (Coy.) as follows:
- combat subunits: 3 tank companies (3 Tk. Coy. x 14 Tk. + 2 Tk. battalion command, total 44 tanks);
- support subunits: 1 combat support company (CS Coy.) and 1 Combat service support company (CSS Coy.). The organisation of these two companies is like the one presented to the tank battalion by branch units, *version no. 1*.

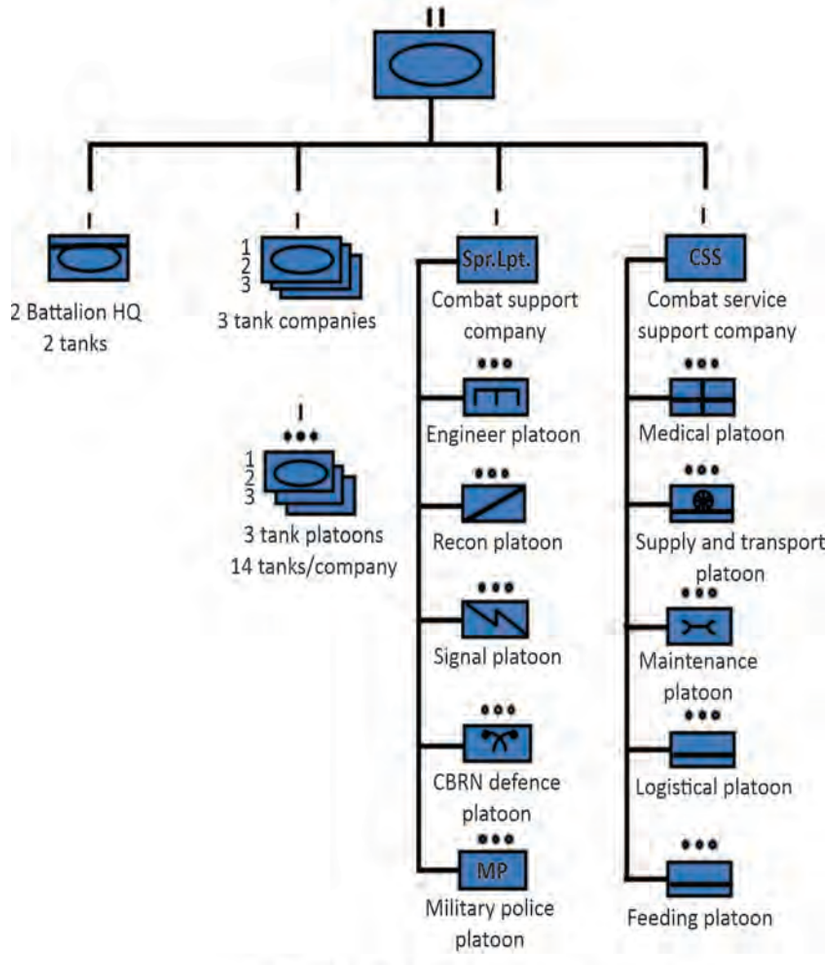


Figure no. 5: Organisation of the tank battalion by branch units, version no. 3.

This tank battalion-like structure on branch units can be found in mechanised brigades or within a tank brigade structure. The organisation of the tank battalion by branch units, *version no. 3*, is shown in *figure no. 5.*

- tank brigade (Tk. Bde.) organised in the following structures:
  - combat structures: 3 tank battalions and 2 infantry battalions, (3 Tk. Bn. x 44 Tk., total 132 tanks and 2 Inf. Bn. x 44 IFV, total 88 IFV);
  - support structures: 1 artillery battalion (Arty. Bn.), 1 antiaircraft defence battalion (AAD Bn.), 1 combat service support battalion (CSS Bn.);
  - brigade subunits: 1 reconnaissance company (Recce. Coy.), 1 engineer company (Engr. Coy.), 1 electronic warfare company (EW Coy.), 1 signal company (Sign. Coy.), 1 CBRN defence company (CBRN Def. Coy.) and 1 combat service support (CSS Coy.).

The organisation of the tank brigade by branch units, *version no. 3*, is shown in *figure no. 6.*

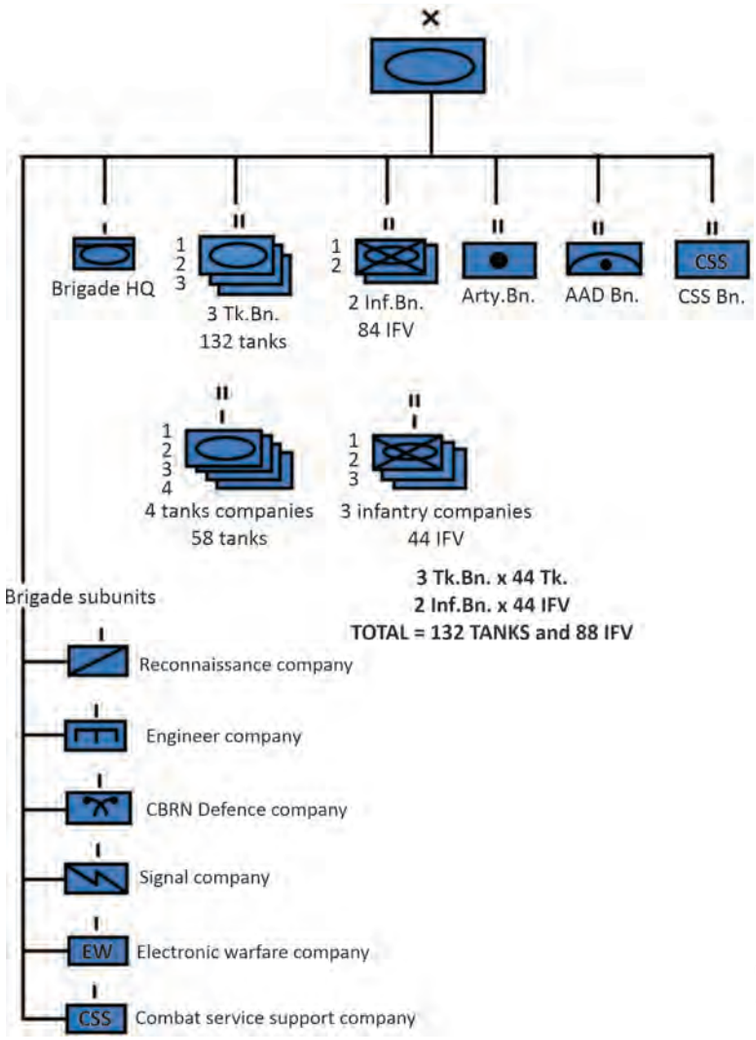


Figure no. 6: Organisation of the tank brigade by branch units, version no. 3.

Modular organisation, subunits of tanks and infantry

The modular organisation would suppose the following constitution:

a. Version no. 1

- tank platoon (Tk. Pl.) organised in 4 tanks (Tk.) one of which is the platoon commander;
- infantry platoon (Inf. Pl.) organised in 4 IFV one of which is the platoon commander;
- tank company (Tk. Coy.) organised in 3 tank platoons (3 Tk. Pl. x 4 Tk + 2 Tc. company command, total 14 tanks);
- infantry company (Inf. Coy.) organised in 3 infantry platoons (3 Inf. Pl. x 4 IFV + 2 IFV company command, total 14 IFV);
- modular armoured battalion organised in 6 companies as follows:
  - combat subunits: 2 tank companies (2 Tk. Coy. x 14 Tk. + 1 Tk. battalion command, total 29 tanks) and 2 infantry companies (2 Inf. Coy. x 14 IFV + 1 IFV battalion command, total 29 IFV);
  - support subunits: 1 combat support company (CS Coy.) and 1 Combat service support company (CSS Coy.).
- the combat support company has the following 5 structures of the level platoon in the composition: reconnaissance, engineer, signal, CBRN defence and military police platoons;
- the combat service support company has the following 5 structures of the level platoon in the composition: medical, supply and transport, maintenance, logistical and food platoons.

This modular armoured battalion structure can be found in mechanised brigades or infantry divisions. Modular organisation of the battalion on subunits of tanks and infantry, *version no. 1*, is shown in *figure no. 7*.

- modular mechanised brigade organised on the following structures:
  - combat structures: 4 modular armoured battalions, (116 Tk. and 116 IFV);
  - support structures: 1 artillery battalion (Arty. Bn.), 1 antiaircraft defence battalion (AAD Bn.), 1 combat service support battalion (CSS Bn.);
  - brigade subunits: 1 reconnaissance company (Recce. Coy.), 1 engineer company (Engr. Coy.), 1 electronic warfare company (EW Coy.), 1 signal company (Sign. Coy.), 1 CBRN defence company (CBRN Def. Coy.) and 1 combat service support (CSS Coy.).

Modular organisation of the mechanised brigade in tanks and infantry subunits, *version no. 1*, is shown in *figure no. 8*.

b. Version no. 2

- tank platoon (Tk. Pl.) organised in 5 tanks (Tk.) one of which is the platoon commander;

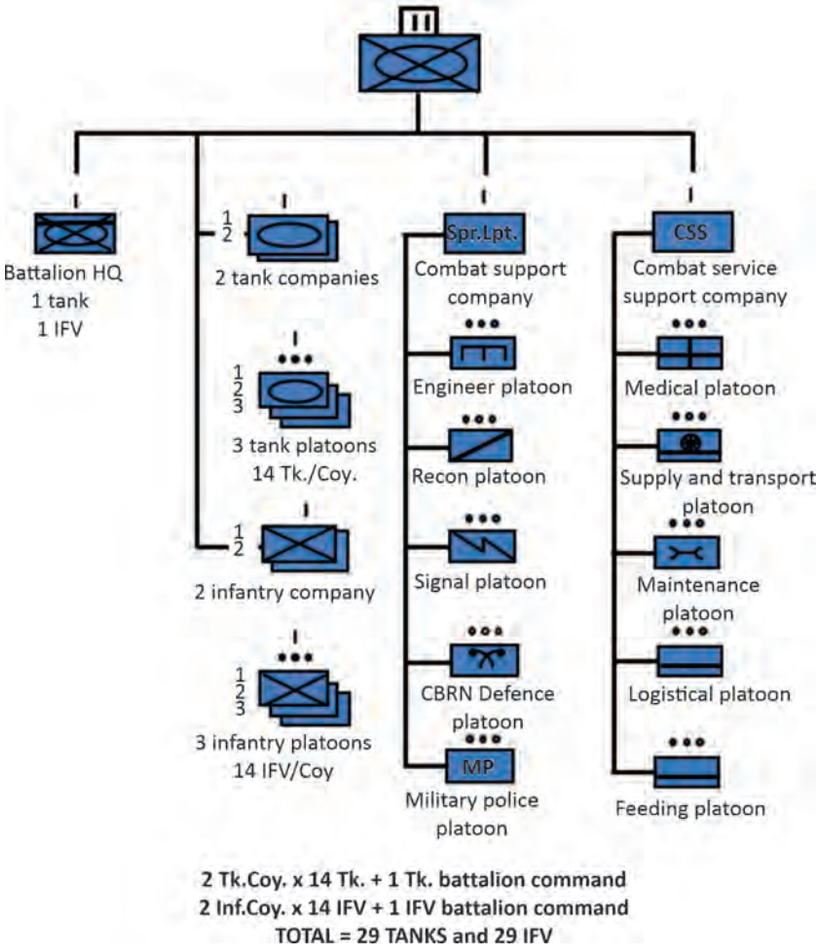


Figure no. 7: Modular armoured battalion structure, version no. 1.

- infantry platoon (Inf. Pl.) organised in 4 IFV one of which is the platoon commander;
- tank company (Tk. Coy.) organised in 3 tank platoons (3 Tk. Pl. x 5 Tk + 2 Tc. company command, total 17 tanks);
- infantry company (Inf. Coy.) organised in 3 infantry platoons (3 Inf. Pl. x 5 IFV + 2 IFV company command, total 17 IFV);
- modular armoured battalion organised in 6 companies as follows:
  - combat subunits: 3 tank companies (3 Tk. Coy. x 17 Tk. + 2 Tk. battalion command, total 53 tanks) and 1 infantry company (1 Inf. Coy. x 17 IFV + 1 IFV battalion command, total 18 IFV);

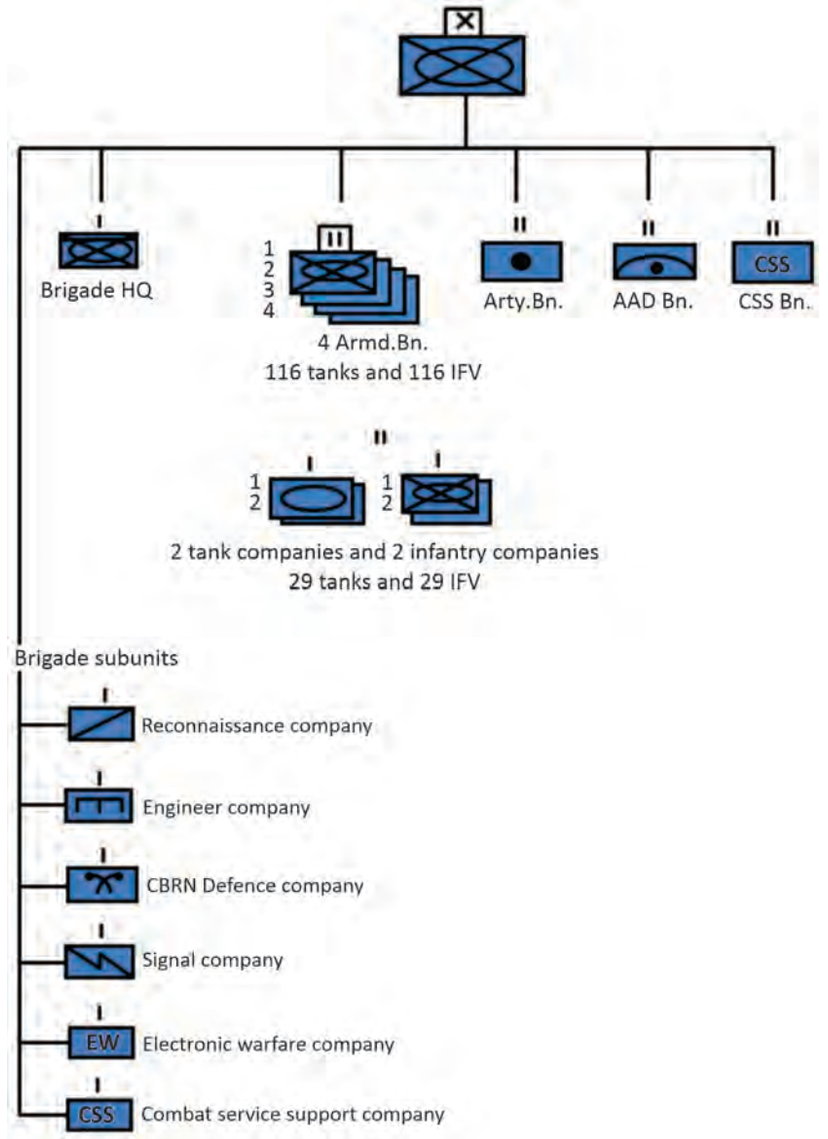


Figure no. 8: Modular armoured brigade structure, version no. 1.

- support subunits: 1 combat support company (CS Coy.) and 1 Combat service support company (CSS Coy.). The organisation of these two companies is like the one presented to the modular armoured battalion, *version no. 1*.

This modular armoured battalion structure can be found in mechanised brigades or infantry divisions. Modular organisation of the battalion in tanks and infantry subunits*, version no. 2*, is shown in *figure no. 9*.

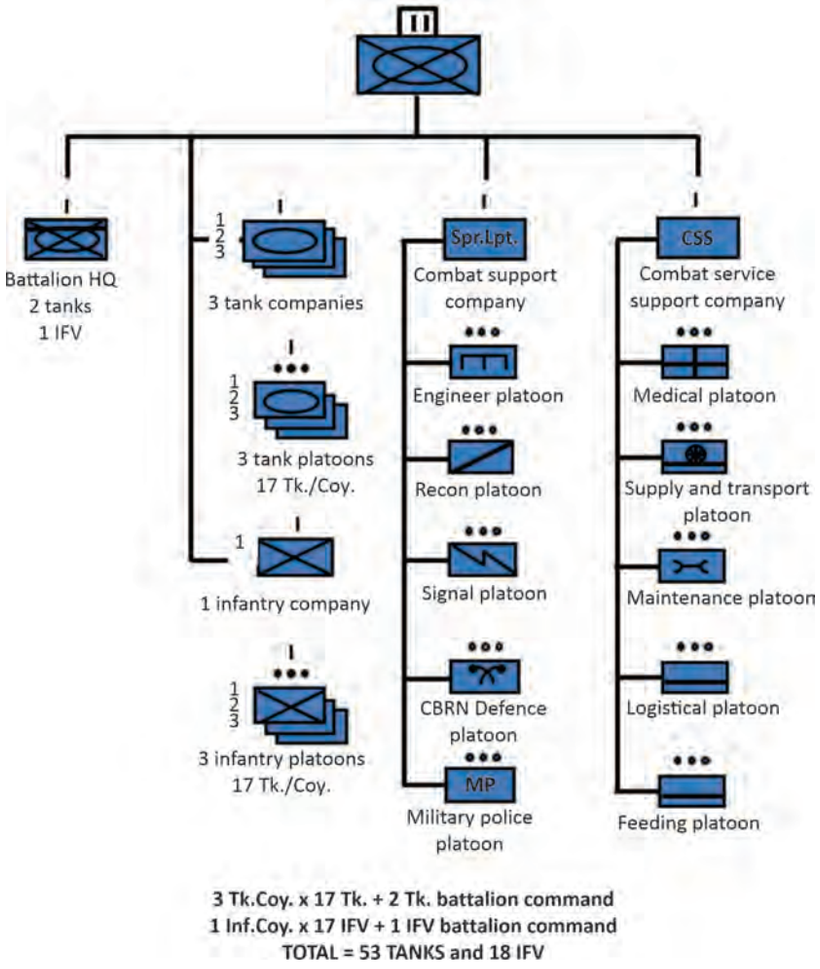


Figure no. 9: Modular armoured battalion structure, version no. 2.

- modular mechanised brigade organised in the following structures:
  - combat structures: 4 modular armoured battalions, (212 Tk. and 72 IFV);
  - support structures: 1 artillery battalion (Arty. Bn.), 1 antiaircraft defence battalion (AAD Bn.), 1 combat service support battalion (CSS Bn.);
  - brigade subunits: 1 reconnaissance company (Recce. Coy.), 1 engineer company (Engr. Coy.), 1 electronic warfare company (EW Coy.), 1 signal company (Sign. Coy.), 1 CBRN defence company (CBRN Def. Coy.) and 1 combat service support (CSS Coy.).

Modular organisation of the mechanised brigade in tanks and infantry subunits, *version no. 2*, is shown in *figure no. 10*.

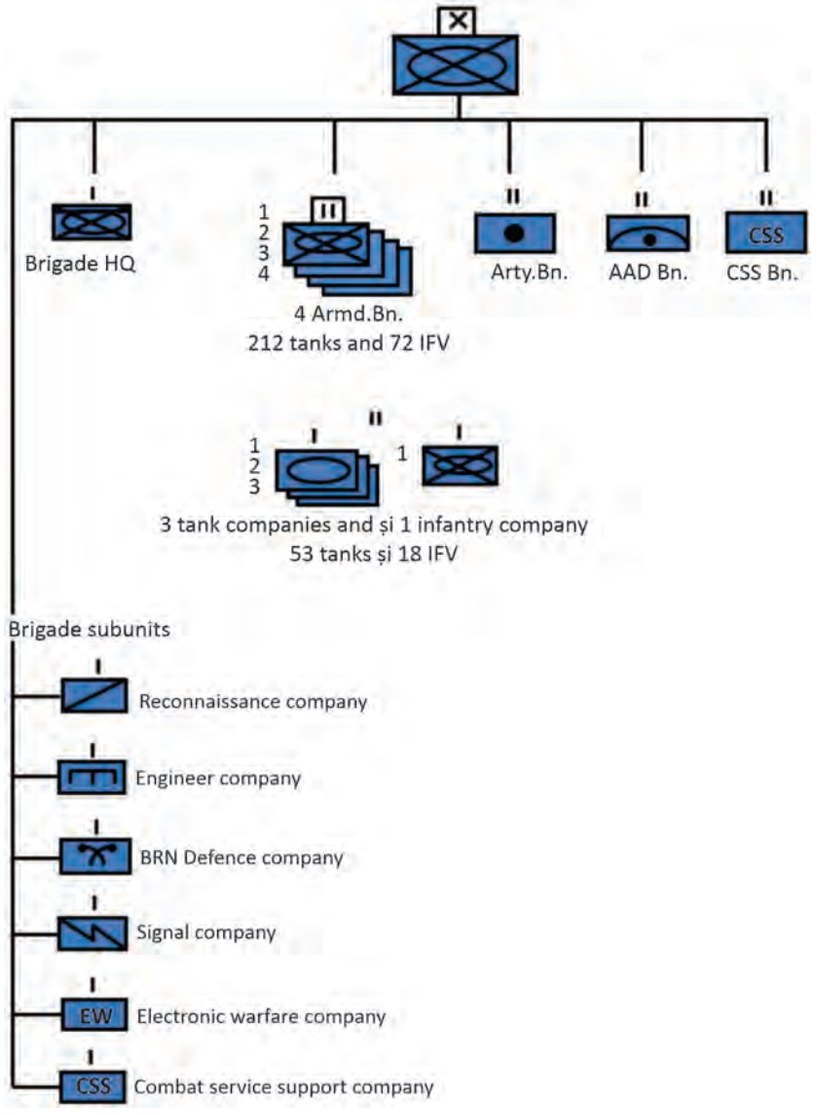


Figure no. 10: Modular armoured brigade structure, version no. 2.

We consider that in the composition of the modular structures there should be armoured vehicles on tracks, tanks and infantry fighting vehicles with similar mobility, as well as subunits for combat support and high mobility logistics support.

We believe that the model of the tank, as well as that of the infantry fighting machine that is part of the equipment of the modular structures, should be from

some NATO member countries, possibly the European Union, their acquisition depending on the life cycle costs of these armoured vehicles and the army readiness to support them.

The advantage of establishing modular structures of brigade level is the fact that, depending on the operational needs and the missions received, armoured groups can be formed only from tanks that aim to increase the fighting power, increase protection and support through fire, execute operations in – fast pace, at the right place and at the right time and with minimal losses.

The Romanian Armed Forces services, land, air and naval, enable the establishment of a group of forces, capable of planning and executing the country defence on the national territory. The lack of a large tank brigade tactical unit forces military planners to adopt solutions that are not exactly in accordance with certain principles, techniques, tactics and procedures for organising a mobile defence, preparing and conducting offensive responses or carrying out actions of freeing some forces that are encircled.

CONCLUSIONS

The process of transformation and modernisation of the Romanian Armed Forces required the land forces structure review. Thus, from large division-level tank units, in 2007, there were only three battalions within the land forces. Subsequently, in the last quarter of 2009, by setting up two other battalions, the current number, namely five tank battalions, was reached. But the establishment of the two battalions was carried out with tanks and other military equipment stored, for at least four years, in the storage centres set up as a result of the reorganisation of the armed forces. Also, the tanks of the three battalions existing at the beginning of 2009 are not of recent generation.

In our opinion, the future tank structures of the Romanian Land Forces will depend on the characteristics of the future tank that will equip this service, which must be interoperable with those of the NATO member states armed forces and become a truly versatile, resistant, capable, strong, but also a very mobile fighter.

The analysis of the physiognomy of the future operational environment and of the threats posed to it is a mandatory condition for determining the future directions of development and reorganisation of the tank structures within the land forces.

We consider that the future Romanian Land Forces tank structures will be determined by two basic courses of action regarding the development and improvement of the tanks, as follows:

- manufacture/purchase of new types of tanks;
- modernisation of existing models.

Currently, we believe that building a new main battle tank of the Romanian Land Forces in our country, in keeping with those existing in other NATO member states, is a challenge very difficult to achieve even though, in the past years, we have been among the few countries in the world that have built tanks.

In our opinion, when choosing to design and build a new main battle tank, it is necessary to develop a common chassis for all armoured vehicles intended for artillery, anti-aircraft defence, chemical, biological, radiological and nuclear defence systems. Thus, designing and building a universal combat platform will be used as a common chassis for the construction of several armoured vehicles, a main battle tank, an armoured infantry vehicle, an engineering vehicle, an armoured evacuation-repair vehicle, a heavy armoured personnel carrier and several types of self-propelled combat vehicles.

Another solution would be to purchase a model in use from a NATO member country. In this situation, the costs of purchasing, providing ammunition, training and maintenance costs appear.

Budget limitation remains the biggest challenge for reorganising tank structures. We consider that the best option, which does not require a long time if supported by a high budget, is the reorganisation of the tank structures through the acquisition of a vehicle that is already part of the procurement of NATO member states, to ensure the interoperability of these members.

BIBLIOGRAPHY

1. SMG-103, *Doctrina Armatei României*, București, 2012.
2. SMFT-10, *F.T.-1, Doctrina operațiilor forțelor terestre,* București, 2017.
3. Asher H. Sharoni, Lawrence D. Bacon, *The Future Combat System (FCS). A Technology Evolution Review and Feasibility Assessment*, in *Armor*, July-August 1997, pp. 7-13.
4. Toma Pleşanu, *Organizarea generală a blindatelor*, Editura A.T.M., Bucureşti.
5. http://www.liveleak.com/view?i=1f9_1363442218
6. http://www.liveleak.com/view?i=1f9_1363442218#PqqBwc7dYIosIUtj.99
7. http://www.liveleak.com/view?i=e51_1399489519
8. http://www.army-technology.com/features/feature-the-worlds-top-10-main-battle-tanks/
9. http://www.cfc.forces.gc.ca/259/290/289/286/lamontagne.pdf#page=2
10. http://www.militaryaerospace.com/topics/vetronics.htm
11. http://www.militaryaerospace.com/articles/2014/02/army-tank-buy.html.
12. http://www.globalsecurity.org/military/systems/ground/fcs-mgv-p.htm
13. http://www.businessinsider.com/11-incredible-weapons-that-only-america-has-2011-9?op=1#ixzz34GEVzcyB
14. http://www.armyrecognition.com/russia_russian_army_tank_heavy_armoured_vehicles_u/armata_russian_main_battle_tank_technical_data_sheet_specifications_information_description_pictures.html#top

A STUDY ON THE CAPABILITIES OF UNCONVENTIONAL OPERATIONAL ELEMENTS, THE CENTER OF GRAVITY OF HYBRID THREATS

Costinel Nicolae MAREȘI
PhD Candidate, "Carol I" National Defence University, Bucharest

By resorting to research techniques such as the content analysis technique, the documentary analysis and the case studies, the scientific research results presented in this article bring to the attention of the specialists novelty elements about the center of gravity of the hybrid threats, through a comprehensive and immersive approach to the current challenges to the international security environment.

The tactics of special operations forces (which are characteristic to states) and irregular forces such as non-state paramilitary forces are treated: insurgents, guerrillas, terrorist groups, mercenaries, private military companies, cross-border criminal organisations, but also other unconventional means: psychological operations, informational operations and cyber aggressions. All of these are treated as structural elements of hybrid threats.

Essentially, in order to prevent or control national security risks posed by hybrid threats, the place and role of unconventional operational elements within these types of emerging threats must be understood. The scientific research in this field requires that the Romanian army is synchronised with the new evolutions of the contemporary war.

Keywords: hybrid threat, private military campaigns, mercenaries, psychological operations, cyber aggression.

INTRODUCTION

The definition given by NATO since 2018 for the hybrid threat is as comprehensive as it is simple, *a threat combining in time and space, conventional, unconventional and asymmetric activities*[1].

The unconventional term covers a wide range of possibilities, but I believe that the most important feature is that unconventional operative elements are those that are not governed by international laws, laws of war or national laws.

Military thinking trends also include weapons of mass destruction in the category of unconventional means, but I believe that these are not the subject of this study because in the hybrid conflicts nominated by specialists and which we have analysed, I have not met their use, nor they are seen them as part of a hybrid opponent's arsenal, which pursues low-intensity conflicts at the boundary between peace and war.

Depending on the operational environment, I propose the following taxonomy for the unconventional structural components of a hybrid threat: the unconventional paramilitary component (frontier, physical environment), virtual unconventional (psychological environment, and non-conventional mixed (with extensive capabilities in several operational environments).

PARAMILITARY UNCONVENTIONAL COMPONENT

The unconventional paramilitary component of hybrid threats refers to paramilitary forces, combatants who are not members of the regular armed forces and carry out irregular actions, fulfilling their goals through indirect action and asymmetric tactics.

Paramilitary forces represent forces or groups, distinct from the regular armed forces of any state, but similar to them as organisation, equipment, training and/or missions[2].

Non-state paramilitary forces can be the insurgent forces, guerrillas, terrorists, mercenaries, private military companies, independent fighters and transnational criminal organisations.

[1] ***, *NATO Glossary of Definitions and Terms*, *AAP-06*, 2018, p. 62.
[2] ***, TC 7-100, *Hybrid Threat*, Washington, 2010, p. 2-5.

Insurgents, terrorists and guerrilla forces

The term insurgents was the name given to American settlers who stood up against England in the 18th century. Insurgency (insurrection) is *a form of armed combat, aiming to oust the existing political regime or an occupying army; riot, uprising*[3].

Terrorists can be insurgent forces, by fighting against the political regime, the authorities in general, or simply are vectors of ideology, religion, or other beliefs that use violence against non-combatant targets. Thus, the Nipponese terrorists behind the sarin gas attack of 20 March 1995 cannot be said to be insurgents. Nipponese members of the religious sect Aum Shinrikyo *("the supreme truth")*, which orchestrated the attack with neurotoxic gas that caused the death of 13 people and the injury of other 5,800 on the three subway buses in Tokyo[4], were pursuing nothing, causing tensions between Japan and external powers, but not the overthrow of legitimate power.

Guerrilla fighters, as a paramilitary force, imply *"military and paramilitary operations carried out by irregular, predominantly indigenous forces, in a hostile/ occupied territory of the enemy"*[5]. Better said, the fight of the occupied one against the invading force, the weak against the strong, the victim against the oppressor. Guerrilla fighters usually are supported by a part of the local population[6].

A point of reference is the taxonomy of violent conflicts presented by Boaz Ganor, *figure no. 1*, from which it can be observed that the unconventional tactics are a *"mirrored"* response of the conventional ones[7].

Mercenaries and private military companies (PMC)

Occupying a leading place, the following on the list of paramilitary forces possible to be the part of a hybrid threat in future conflicts are mercenaries and private military companies.

According to the UN International Convention on recruitment, use, financing and training of mercenaries, which has produced effects since 20 October 2001, *jus in bello*, it states that are illegal all the activities concerning hiring of mercenary

[3] https://dexonline.ro/definitie/insurgenta, retrieved on 15.08.2019.
[4] https://www.bbc.com/news/world-asia-35975069, retrieved on 16.08.2019.
[5] ***, US Department of Defence, *Joint Publications (JP) 3-05.1, Joint Special Operations Task Force Operations*, 2007, p. GL-11.
[6] Valerică Cruceru, *Elemente de artă militară întâlnite în războiul de gherilă modern,* in Buletinul Universității Naționale de Aparare *"Carol I"*, nr. 2/2013, p. 2.
[7] Boaz Ganor, *Defining Terrorism*, International Policy Institute for Counter-Terrorism, 2010.

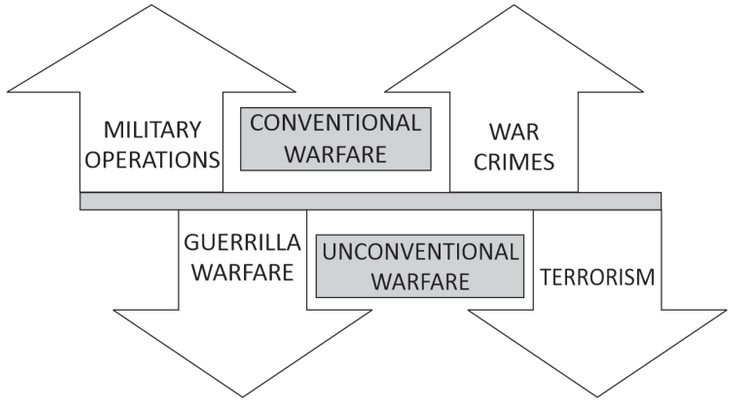


Figure no. 1: Taxonomy of violent conflicts

forces. The definition of a mercenary implies meeting cumulative features. Here is a sum up of the most important ones:

- he is specially recruited in the country or abroad to fight in an armed conflict;
- takes part in hostilities for a personal gain that is promised by a party to the conflict or on its behalf, a higher remuneration than then one promised or paid to combatants having an analogous degree and function in the armed forces of this party[8].

At the time of research, only 35 member countries ratified the convention. Countries such as Russia, USA or United Kingdom, that have high military capabilities have not ratified because they make use of the so-called private military companies.

Private military companies, known as *"private warriors"*, because most of them come from reserve military frameworks, play an important role in technical, technological and logistical support, secure security ambitions, collecting Information, defence training, even active participation in conflicts. Mainly they have a defensive role but not all, as I will give some examples in the following lines. It is again very interesting that they can be employed by both states and companies or even individuals.

Given that these entities do not belong to the states and so they do not obey the Hague Conventions they give a new dimension to violence in an armed conflict.

Two crimes of these actors in conflict zones are well known and heavily mediatized: the opening of fire against the civilian population of Baghdad in September 2007 by the employees of the private military company Blackwater,

[8] http://www.un.org/documents/ga/res/44/a44r034.htm, retrieved on 20.08.2019.

currently Academi, when 17 civilians were killed and many others injured, and also the involvement of the companies CACI International and Titan of San Diego[9] in torturing Iraqi prisoners with CIA and other military employees, in the year 2003-2004 at Abu Ghraib Prison, 30 km west of Baghdad. Representative for the last case are the pictures presented in *figure no. 2*, brought to public attention in 2004.

Private military companies and mercenaries will find themselves more and more in conflict areas, especially as elements of a hybrid threat.

The most vocal use of private military companies in recent hybrid conflicts is linked to the Russian company known as the Wagner Group, *the green men*, which has been involved since the beginning in the conflicts that took place in Crimea and eastern Ukraine, by organising the attacks on Ukrainian administrative institutions, training pro-Russian separatists and active participation in combat, such as the battle of the beginning of 2015 (14 January-20 February 2015) for Debaltseve, an important road and rail node[10].

Major General Sergei Kanchukov, former head of the military intelligence service in the Siberian District and a veteran of the Military Intelligence Service (GRU), said that a combination of advanced equipment and high professional skills, directly controlled by the state, gives the PMC the capability to carry out tasks typically specific to the Russian armed forces. Moreover, he argues that, unlike regular forces, these structures are free to choose any means to achieve their specific objectives[11].

Freelance warriors

Regarding the foreign fighters, *freelance warriors* (freelance, independent), which I consider a niche paramilitary force, there is no internationally accepted legal definition and no legal framework for their activity. They are people who leave their country of origin or habitual residence and engage in violence as part of an insurgences or a partisan armed group in an armed conflict. They are motivated by a number of factors, especially ideology, but can also be attracted by financial reward, such as the one that is brought by preying on the remains found in the war zones[12].

According to UATV, an international audio-visual multimedia platform in Ukraine, in November 2017, about 100 foreign fighters, partisans of the regime in Ukraine,

[9] https://corpwatch.org/article/private-contractors-and-torture-abu-ghraib-iraq, retrieved on 19.08.2019.
[10] http://euromaidanpress.com/2019/03/02/ukrainian-ngo-collects-data-on-1500-russian-wagner-mercenaries-in-operation-trust-remake/, retrieved on 19.08.2019.
[11] https://www.researchgate.net/publication/328450701_'Continuing_War_by_Other_Means'_The_Case_of_Wagner_Russia's_Premier_Private_Military_Company_in_the_Middle_East, retrieved on 15.08.2019.
[12] https://www.globalsecurity.org/military/world/para/mercenary.htm, retrieved on 19.08.2019.

were taking part in actions with the regular forces. Among these fighters there were citizens of Belarus, Georgia, Lithuania, Republic of Moldova or even Russia[13].

Privatisation of war could become a state policy for a state that wants to projects its force outside its borders, but whose citizens are not willing to shed blood. An enlightening example is that at one point the private military companies accounted for about 50% of the forces employed by the US in Iraq and 55% in Afghanistan[14].

Transnational criminal organisations

According to the UN Convention against organised cross-border crime (UNTOC)-the Palermo Convention of 15 November 2000, which entered into force in 2003, which also has three protocols[15], ratified by the majority of states, the definition of organised criminal group is: *a "structured group of three or more persons, who exist for a certain period and act in agreement, for the purpose of undertaking one or more offenses predicted by the present convention, in order to obtain, directly or indirectly, a financial advantage or other material advantage"*[16].

The activities of these criminal organisations are limited to: money laundering, corruption, smuggling, acts of violence (on persons or property – vandalism and destruction). There are also special forms of criminality with a cross-border component such as terrorism, human trafficking and cybercrime[17].

I wish to highlight two things on this subject, namely cybercrime and transnational mafia-type criminal organisations, whose share in hybrid threats will increase significantly in the future.

Modus operandi of cybercrime is constantly evolving, cutting its way to the first position in the top of the most dangerous threats to national security.

Russian-speaking cyber attackers are prominent in this area of crime. Their targets tend to become service providers to the detriment of individual users, because having access to their database, they can gain access to the confidential data of their customers.

[13] https://www.youtube.com/watch?v=X7r-LvsWUfg, interview retrieved on 21.08.2019.
[14] https://aeon.co/essays/what-does-the-return-of-mercenary-armies-mean-for-the-world retrieved on 10.08.2019
[15] The Protocol on the prevention, suppression and punishment of trafficking in human beings, in particular women and children, the Protocol against illegal smuggling of migrants by land, by air and by sea, and the Protocol against the manufacture and trafficking of illicit firearms, parts and components for them and ammunition.
[16] ***, The UN Convention against Organised Cross-border Crime (UNTOC), art. 2, para (a), translated at http://www.monitoruljuridic.ro/act/conventia-natiunilor-unite-din-15-noiembrie-2000-impotriva-criminalitatii-transnationale-organizate-emitent-organizatia-natiunilor-unite-publicat-n-39751.html, retrieved on 10.08.2019.
[17] https://rm.coe.int/cartea-alba-a-criminalitatii-organizate-transnationale/168070ab40, retrieved on 10.08.2019.

Most likely they will orient themselves to attack critical infrastructure[18], an well-known example of this statement being the "*Stuxnet*" virus, revealed in the year 2010, designed to harm the nuclear facility in Natanz (Iran) by modifying valves' opening and closing rhythm affecting the supply with hexafluoride gas, that was required by centrifuges to enrich uranium[19].

As to mafia-type transnational criminal organisations, the members of the biker group "*night's wolves*", nicknamed as *"Putin's angels"*, seem to be already considered an unconventional component of a hybrid threat like Russia. Voices of the US central administration say they are collaborating with special forces in the Kremlin, recruiting separatists and being directly involved in conflicts in the Donetsk and Luhansk regions, including the siege of Ukrainian naval forces' facility based in Sevastopol.

Their leader is Alexander Zaldostanov, "*the surgeon*", a companion of Russian's president, with which he was seen at several ultranationalist Russian events in both Russia and Ukraine[20].

Recently they created a genuine military base, on the site of a former pig farm in Dolna Krupa village (70km NE of Bratislava) where they hold tanks, armoured vehicles and military equipment, as observed in photos taken in the summer of 2018, with the help of drones. The group leaders argue that they want to build a museum dedicated to the Soviet Army during the Second World War[21].

Transnational criminal groups enjoy increased freedom and at the same time make things difficult for the authorities because they are able to successfully speculate on national and international legislation, they wrongfully make use of the universal rights and freedoms. They also defend themselves by making use of their state-level sponsors' reputation. For the above mafia-type transnational criminal group the Slovak central administration must be careful that their eventual interventions in the group, activities not to affect the diplomatic relations with Russia.

I will review several names of the most powerful cross-border criminal organisations: Solntsevskaya Bratva (involved in drug trafficking from Afghanistan), Yamaguchi Gumi-*"yakuza"*, Camora, Ndrangheta, the Sinaloa cartel, each of them with a capital exceeding 3 billion dollars[22].

[18] https://www.europol.europa.eu/content/eu-seroius-and-organised-crime-threat-assessment-socta, Raport Europol SOCTA 2013, *Evaluarea amenințării legate de crima organizată,* retrieved on 13.08.2019.
[19] ***, *Spionii, cine sunt și ce fac? O incursiune în spionajul contemporan*, Editura RAO, București, 2013, pp. 347-348
[20] https://www.bbc.com/news/world-europe-45019133, retrieved on 13.08.2019.
[21] https://www.rferl.org/a/night-wolves-putin-bikers-slovakia-military-camp-/29385437.html, retrieved on 13.08.2019.
[22] http://fortune.com/2014/09/14/biggest-organized-crime-groups-in-the-world/, retrieved on 16.08.2019.

There are specialised opinions that suggest "*organised crime constitutes a parallel economic system, which achieves business figures and illegal benefits that exceed in some countries, their gross national product*"[23].

Since both insurgency groups (guerrilla) and criminal organisations outside the law, and anti-government, there are situations when they cooperate for mutual support.

In Colombia, where the local mafia from Medelina and the Gulf Clan (Urabenos) operates, according to a UN data report, there are approximately 171,000 hectares cultivated with coca plants[24]. There is a durable collaboration between them and guerrilla forces partisan to the regime, AUC (United Self-Defense Forces of Colombia -currently demobilised)[25] and also with the dissident forces FARC (Revolutionary Armed Forces of Colombia – Marxist ideology), whih perceived commissions on the drug trade practiced on their territory.

Huge revenues from illegal drug trafficking allow insurgents and partisans to supply themselves with weapons, equipment and human resources, while providing shelter for criminal organisations in rural areas that they control[26].

According to the sources cited above, things are gaining a new critical dimension, when during FARC demobilisation, the Mexican cartel Sinaloa intervenes, eager to take over the black drug market in Colombia, rearms the FARC leaders and imposes their authority in the Colombian port city Tumaco[27].

The above example is not just a scenario, it is the reality facing a sovereign state. This symbiosis between the elements of organised crime and the insurgents or partisans creates a genuine hybrid threat to the national security of a state.

The military experience of paramilitary forces is sought by criminal organisations because they provide security and protection, they offer reconnaissance capabilities, early warning and give them a certain weight to their statute among the rival groups.

[23] https://www.academia.edu/33322781/conceptul_de_criminalitate_organizat%c4%82_%c3%8en_dreptul_european, retrieved on 16.08.2019.
[24] https://www.france24.com/en/20181213-cartels-ex-farc-alliance-poses-new-threat-colombia-hrw, retrieved on 16.08.2019.
[25] https://profiles.colombiareports.com/auc/, retrieved on 16.08.2019.
[26] https://www.wilsoncenter.org/sites/default/files/otis_farcdrugtrade2014.pdf, John Otis, *FARC și comerțul ilegal de droguri din Columbia*, Editura Wilson Center, 2014, retrieved on 17.08.2019.
[27] *Ibid*, p. 35.

VIRTUAL UNCONVENTIONAL COMPONENT

In this chapter, I will present the capabilities of psychological, informational and cyber-attack operations. The first two types of operations, the informational and psychological ones, which are also part of Romania's military capabilities, have a higher influencing power on the civilian population, due to the fact that they are more receptive and non-discriminatory about the information served to them. These operations are the two means used in the battle for perceptions, aimed at altering the will and cancellation of population support for the opponent's armed forces.

Psychological operations

Psychological Operations (PsyOps) are a range of actions targeting the cognitive field aimed at inducing attitudes and behaviours that affect the achievement of the enemy's strategic objectives. Their role is to produce emotions such as hatred, shame, fear, eroding the will of the opponent.

PsyOps rely on manipulation*, "deliberate spread of information, rumours, ideas and works of art, in order to harm other specific groups, movements, beliefs, institutions or governments"*[28].

The first operationalised PsyOps were initiated by the French in 1915, when they established the *"aviation propaganda service"*, then followed Germany and England, which set up the *"propaganda office"*. In 1917, the first bomb with manifests (flyers) was used, which had a capacity of 500 manifests.

A resounding success in recent military history that PsyOps had in the theatre of operations was in the first Gulf War (2 August 1990 – 28 February 1991), before and during the Desert Storm operation, when an international coalition, under the UN flag, fought for the liberation of Kuwait from the newly established occupation by Iraq.

At that moment in time, PsyOps consisted of:

transmitting radio and TV broadcasts, such as the *"Voice of the Gulf"*, allied propaganda, which presented them in a favourable light to induce fear of retaliation, both on conquered territory of Kuwait and also in Iraq. (Plane EC-130E Volant Solo was broadcasting on radio frequencies during the flight deep into the enemy's land).

- using portable speakers on military machines, which transmitted messages of urge to desertion;

[28] Marius Nițulescu, *Operațiile psihologice, necesitate a actului de comandă*, in *Buletinul de teorie militară*, no. 4, Editura SMFT, 2010, http://www.revista.forter.ro/2010_4_t/02-fm/06.html, retrieved on 17.08.2019.

- spreading, with the support of aviation, artillery, of manifests, small pieces of paper with drawings and/or text messages.

The results in figures of the success of psychological operations show that 44% of Iraqi troops deserted, of which almost 87,000 Iraqi troops joined the coalition forces after they found and read the manifests.

Informational operations

Informational operations are a range of military actions aimed at influencing the decision-making process of the opponent to support the achievement of their own objectives, while safeguarding its own informational system. Strategic targets are information, opponent's systems and processes based on information. According to NATO's doctrine, there are 3 pillars on which *InfoOps* rely: *people* – decision-makers, opinion leaders, *hardware systems* (computer networks) and *informational processes* that link the *hardware systems* to the decision-makers, for example organizational structures techniques, tactics, procedures.

Public opinion is informed and manipulated through mass-media, which at the same time, influence the politicians' decisions on strategic level.

Informational attacks involve strategic deterrent operations, misleading (serving the opponent of false intelligence), media warfare.

Although there are factors that help the development of society, multimedia information, exchange technology, the free flow of information, the right to freedom of opinion and expresion, social networks can also be used in other ways, serving hostile intentions.

The media war is *"the confrontation between the mass-media controlled by adversary parties, looking to impose their own version of the causes, the evolution and the consequences of the conflict both to national and also to international audience"*[29]. This kind of war most of the time is based on misinformation, such as fake news. Fake News are a hot topic for profile institutions, because they are widely used by current and rising hybrid threats. The media war is a component of battle for perceptions.

Islamic State (ISIS)[30] has known remarkable successes through the use of the media war. Thanks to the dissemination to the whole world of their acts of terrorism and live images from the assault on Arab cities in Iraq and Syria, they managed to attract an unexpected number of fighters from the war zones and western countries.

[29] Călin Hentea, *Propaganda fără frontiere*, Editura Nemira, București, 2002, p. 24.

[30] Sunnite, salafist and insurgent group affiliated with al-Qaeda, active in Iraq and Syria (leader Abu Bakr al-Baghdadi).

Islamic Propaganda was the second weapon of this hybrid threat. This statement is best represented in *figure no. 2*.

Figure no. 2: A successfully made representation of ISIS propaganda in conflict zones (Front cover of Media operative, You are a Mujahid, Too)

Since April 2016, in the virtual environment circulated a propaganda material belonging to ISIS, called the *Media operative, You are a Mujahid, Too*, which was practically an official recognition of the importance of the informational war for their jihad.

By calling for ideological, theological (religious) and emotional reasons, they urged to support their cause by spreading propaganda by any volunteer, recognizing its importance equally to that of the fighter who actually was engaged in the military conflict.

The idea that this kind of support force is very important is not new, as described in the above-mentioned publication. Usamah bin Ladin said in 2002 that it was *"a group of media operators and comrades of the pen who have a prominent role in directing the war, destroying the enemy's morale and raising the spirits of Muslim communities*".

Media combatants had to follow three main lines of effort: a positive narrative (Islam as the opportune alternative), arguing with adversaries and operationalising the media to serve them[31].

Social networks after the televised media are the environment in which mass opinion is build. Here the informational warfare is conducted with fake accounts and robotrolling[32].

[31] https://www.stratcomcoe.org/media-jihad-islamic-states-doctrine-information-warfare, Charlie Winter, *Media Jihad: The Islamic State's Doctrine for Information Warfare*, retrieved on 21.08.2019.

[32] Transmission of repugnant messages intended to produce discord between their readers.

Russia has speculated this vulnerability of states' security, represented by online social media platforms. As Aristotle said in "*Politics*", "*man is by nature a social being"*. In his groups, he learns, develops new features, is strong but also vulnerable.

A spearhead in the informational warfare, deeply active behind enemy lines, with connections to the intelligence service of the Russian army[33] (acronym GRU), is the newly known Internet Research Agency (IRA), *"Trolls from Olgino"*, based in Saint Petersburg.

Founded in 2013, this puppet institution served high-stakes interests for the Kremlin in the 2016 presidential elections in America. Through their manipulation and disinformation campaign, they proved to have knowledge of the delicate topics in the American society and culture, which they exploited, in the virtual environment, in an organised and maximum efficiency manner.

IRA's trolling campaign rested on topics that created a lot of tension between voters: the right of Americans to hold personal weapons, police abuses, the black community social issues (racial segregation), the secession between North and South (#Texit, #Calexit), the issue of immigrants, conspiracy theories, electoral frauds, the war in Syria.

Memes, those ideas that quickly propagate into a culture, were the centre of gravity in the informational operations undertaken by the IRA in America

Social robots are computer programming algorithms that mimic human behaviour.

Between 1 May and 31 July 2018, 49% of all Russian messages related to NATO's presence in the Baltic and Polish countries were created automatically. Of the total accounts on social networks belonging to Russian-speaking accounts, this kind of messages accounted for 36% of the all of them[34].

Informational operations are a vital component of hybrid threats, especially because they are very effective against the civilian population, which is easy to influence, thus serving the strategic interests of someone else without knowing.

Cyber-attack operations

An unconventional mean that I believe will dominate among the other elements of a hybrid threat are cyber-attacks.

[33] Name changed in the year 2010, in the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, known under the acronym GRU, according to https://www.reuters.com/article/us-britain-russia-gru-factbox/what-is-russias-gru-military-intelligence-agency-idUSKCN1MF1VK, retrieved on 15.08.2019.

[34] https://www.stratcomcoe.org/robotrolling-20183, *Rotrolling*, NATO Strategic Communication Centre of Excellence, Riga, retrieved on 23.08.2019.

It is a tool within the reach of states, but also of non-state actors (transnational criminal organisations, individuals, insurgent groups) that originally appeared in the civilian environment, but quickly spread into the military domain.

State entities that assume their role as aggressors in cyberspace are countries such as North Korea, China and Russia use such tactics because it is a relatively new area, which does not have a system of incrimination and strong coercive measures in international law.

Relevant to the integration of cyberspace into the international law system is the *"Tallinn Handbook"*, that already reached the second edition, a product of the NATO Cooperative Excellence Centre for Cyber Defence (21 member states in 2018)[35] which was built in 2008 in Estonia, one year after Russia's cyber-attacks on this country. The role of this military institution is purely defensive.

Because cyber attackers leave little *"footprints"* or not at all, it is hard to issue accusations against attackers. No country recognises its operations in cyberspace. Because it is hard to prove that someone did a cyber-attack, they are inevitably used in a hybrid conflict.

The targets of cyber-attacks can be any entity operating in cyberspace (virtual), but there are preferred by attackers valuable targets for national security such as state institutions, critical infrastructure, political deciders, banks.

Cyber-attacks from Russia's side are an enlightening component in seeing it as a hybrid threat to the international order and security.

On the timeline presented in *figure no. 3*, in the last decade, Russia cyber assaulted ex-Soviet countries thereby trying to bring these countries under its influence, while an integration of cyber-attacks into broader joint operations can be seen.

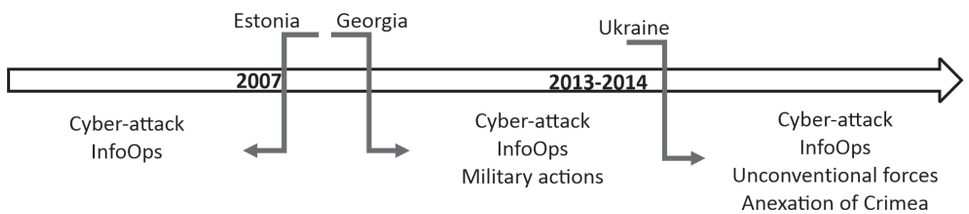


Figure no. 3: Integration of cyber-attacks into military operations led by Russia in the space of former USSR

[35] https://ccdcoe.org/research/tallinn-manual/, retrieved on 12.08.2019.

The Bronze Soldier crisis in Tallinn began on 26 April 2007, when the Estonian authorities began the preparations to relocate this Soviet monument from the Second World War from the centre of Tallinn to a military cemetery. The moment was speculated by the Kremlin authorities for assaulting the Estonian state.

The attacks began with the transmission of a large amount of messages on mobile phones in Estonia to disseminate disinformation, urging the Estonian population to start an armed resistance against the government. The Russian media urged volunteers to launch cyber-attacks against Estonian political parties and government sites, providing lists of objectives, instructions and response tools. The classic DoS and DDoS attacks followed[36], reaching attacks targeting critical informational infrastructure-domain naming servers (DNS), network nodes of telecommunications companies. These actions resulted in the collapse of telephone communications for certain periods of time, disruption of government sites and banks. It was estimated that the most important bank in Estonia suffered damage of over 6 million euros.

The armed conflict between Georgia and Russia, from August 2008, started as a result of Georgia's military intervention over the separatist South Ossetia region. Cyber-attacks coincided with Russia's military intervention in South Ossetia, 8-9 August 2008. Russia launched DDoS's attacks on government websites, compromising them, mass spammers, breaking email accounts, disclosing private information to the general public and various malicious elements that previously have been suggested on Russian forums (StopGeorgia.ru, Xakep.ru), things like lists of targets, instructions and cyber-attack tools against Georgians being distributed.

As for Ukraine, the number of DDoS attacks, compromising Ukrainian sites, sending SMS containing pro-Russian propaganda has risen significantly since December 2013.

In March 2014, Russia executed military operations supported by cyber-attacks against Ukraine, a DDoS attack 32 times more virulent than those previously used in Georgia, interrupted the internet in this country while pro-Russian rebels took over the control of the Crimean Peninsula[37].

In December 2015, the Ukrainian authorities informed that cyber-attacks on the national energy system were those that left over 200,000 private consumers in the dark for hours in a row. In 2016, various cyberattacks were launched on the Ukrainian critical infrastructure (Kiev electrical network, Kiev Airport, Treasury,

[36] Denial of Service and Distributed Denial of Service.

[37] https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111, retrieved on 11.08.2019.

Pension Fund, etc.). The most extensive economic damage was conducted with *NotPetya ransomware* in June 2017, which disabled 10% of computers in Ukraine and caused financial losses of 0.5% of Ukraine's GDP. Ukrainian intelligence services accused the Russian government of being behind these attacks.

Cyber-attacks in support of informational operations launched by Russia tend to be increasingly geared towards fraud or influencing electoral elections in democratic states, in order to ensure the reach to power of Kremlin's favourite candidates.

MIXED UNCONVENTIONAL COMPONENT

Special operations forces (*SOF)* are the mixed unconventional component, as they operate both in the physical environment and in the psychological and informational environment. They can act both conventionally, albeit more rarely, but also unconventionally.

The mission of *SOF* in the American vision involves counterinsurgency tasks, counterterrorism, informational operations, unconventional warfare, direct actions (short, precise missions), preparing the defence of the states where they are deployed, special reconnaissance, assisting in force protection[38]. Their operations are specific, quick, surgical, small-scale aimed at enemy forces' centre of gravity (*COG*), liquidation of leaders, destroying targets of strategic importance, and so on.

SOF can also be involved in training insurgents on how to exploit vulnerabilities, by training them regarding tactics, techniques and procedures for the purpose of producing major damage and psychological effects on opponents. *SOF* can easily infiltrate the local population of the conflict area, understanding their specific cultural, historical and ideological identity, by voluntarily directing their actions to serve the purposes imposed by the states of which they belong.

The involvement of Russian *SOF* in recent conflicts in Ukraine is heavily investigated by specialists and all conclusions urge to recognise the crucial role they have had in the evolution of events.

CONCLUSIONS

Through this study, I approached theoretically and practically, with conclusive examples of hybrid conflicts, the capabilities of unconventional means integrated into the hybrid operations of adversaries.

[38] ***, FM 3-05.20 (FM 31-20), *Doctrine for special forces operations*, 2001, p. 2, https://fas.org/irp/doddir/army/fm3-05-20.pdf, retrieved on 11.08.2019.

A hybrid threat poses a greater risk to national and international security proportional to the unconventional elements incorporated. Given this consideration, I propose the following classification:

- *Grade 0 hybrid threat* – contains elements of the same group of unconventional means, specifically the hybrid threat from Colombia constituted by FARC-insurgents (paramilitary forces) and drug cartels (transnational criminal organisation);
- *Grade 1 hybrid threat* – contains unconventional elements from two groups of unconventional means, for instance Hezbollah, consisting of insurgents (paramilitary forces) and other unconventional elements-informational operations;
- *Grade 2 hybrid threat* – contains distinct types of unconventional elements from all groups of unconventional means, such as Russia in the recent conflicts with Ukraine, consisting of insurgents (pro separatists Russian-paramilitary forces), Russian *SOF* and other unconventional elements: cyber-attacks, informational and psychological operations.

The different types of hybrid threats impose countermeasures tailored to their specificities. These unequivocally could be a subject for new scientific research.

While conventional military operations are a constant and mandatory condition to discuss a hybrid threat, unconventional force elements can be used in different ways, but synchronously with the first.

I conclude with the assertion that the hybrid threat is a system of conventional and unconventional threats, in which the share is held by unconventional ones.

According to systems theory, a system is more than the sum of its pieces, because there are relations that arise between them and alter the ratio of forces. By analogy, the hybrid threat, which is a system, benefits from that force multiplier resulted from the relations between its elements.

For countering hybrid threats, it is necessary to understand the military and non-military elements of the operational environment, to build an early warning system, to operate in a joint, interagency, multinational framework and to enforce a solid strategic communication leading the civilian population to a critical thinking regarding information that they access.

BIBLIOGRAPHY

1. Valerică Cruceru, *Elemente de artă militară întâlnite în războiul de gherilă modern,* in *Buletinul Universității Naționale de Apărare "Carol I"*, no. 2/2013.
2. Boaz Ganor, *Defining Terrorism*, International Policy Institute for Counter-Terrorism, 2010.

3. Călin Hentea, *Propaganda fără frontiere*, Editura Nemira, Bucureşti, 2002.
4. Marius Nițulescu, *Operațiile psihologice, necesitate a actului de comandă*, *Buletinul de teorie militară*, no. 4, Editura SMFT, 2010, http://www.revista.forter.ro/2010_4_t/02-fm/06.html.
5. ***, Department of Defence, *Joint Publications (JP) 3-05.1, Joint Special Operations Task Force Operations*, 2007, p. GL-11.
6. *** FM 3-05.20 (FM 31-20), *Doctrine for Special Forces Operations*, 2001, p. 2, https://fas.org/irp/doddir/army/fm3-05-20.pdf.
7. ***, *NATO Glossary of Terms and Definitions, AAP-06*, 2018.
8. *** *Spionii, cine sunt și ce fac? O incursiune în spionajul contemporan*, Editura RAO, București, 2013.
9. *** TC 7-100, *Hybrid Threat*, Washington, 2010.
10. ***, *The UN Convention against Organised Cross-border Crime (UNTOC),* art. 2, para (a), translated at http://www.monitoruljuridic.ro/act/conventia-natiunilor-unite-din-15-noiembrie-2000-impotriva-criminalitatii-transnationale-organizate-emitent-organizatia-natiunilor-unite-publicat-n-39751.html.
11. http://euromaidanpress.com/2019/03/02/ukrainian-ngo-collects-data-on-1500-russian-wagner-mercenaries-in-operation-trust-remake/.
12. http://fortune.com/2014/09/14/biggest-organized-crime-groups-in-the-world/.
13. http://www.un.org/documents/ga/res/44/a44r034.htm.
14. https://aeon.co/essays/what-does-the-return-of-mercenary-armies-mean-for-the-world.
15. https://ccdcoe.org/research/tallinn-manual/.
16. https://corpwatch.org/article/private-contractors-and-torture-abu-ghraib-iraq.
17. https://dexonline.ro/definitie/insurgent.
18. https://profiles.colombiareports.com/auc/.
19. https://rm.coe.int/cartea-alba-a-criminalitatii-organizate-transnationale/168070ab40.
20. https://www.academia.edu/33322781/conceptul_de_criminalitate_organizat%C4%82_%C3%8EN_dreptul_european.
21. https://www.bbc.com/news/world-asia-35975069.
22. https://www.bbc.com/news/world-europe-45019133.
23. https://www.europol.europa.eu/content/eu-seroius-and-organised-crime-threat-assessment-socta, Europol SOCTA 2013.
24. https://www.france24.com/en/20181213-cartels-ex-farc-alliance-poses-new-threat-colombia-hrw.
25. https://www.globalsecurity.org/military/world/para/mercenary.html.
26. https://www.hsdl.org/c/tactics-and-tropes-of-the-internet-research-agency/, *The Tactics & Tropes of the Internet Research Agency*¸ New Knowledge.
27. https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

28. https://www.researchgate.net/publication/328450701_'Continuing_War_by_Other_Means'_The_Case_of_Wagner_Russia's_Premier_Private_Military_Company_in_the_Middle_East.
29. https://www.reuters.com/article/us-britain-russia-gru-factbox/what-is-russias-gru-military-intelligence-agency-iduskcn1mf1vk.
30. https://www.rferl.org/a/night-wolves-putin-bikers-slovakia-military-camp-/29385437.html.
31. https://www.stratcomcoe.org/media-jihad-islamic-states-doctrine-information-warfare, *Media Jihad: The Islamic State's Doctrine for Information Warfare,* Charlie Winter.
32. https://www.stratcomcoe.org/robotrolling-20183, *Robotrolling*, NATO Strategic Communication Centre of Excellence, Riga.
33. https://www.wilsoncenter.org/sites/default/files/otis_farcdrugtrade2014.pdf, John Otis, *FARC și comerțul ilegal de droguri din Columbia*, Editura Wilson Center, 2014.
34. https://www.youtube.com/watch?v=X7r-LvsWUfg.

REALITIES AND TRENDS IN THE EVOLUTION OF THE NAVAL CYBERNETIC SECURITY CONCEPT

Sebastian Gabriel POPESCU
PhD Candidate, the Romanian Naval Forces, Bucharest

The analysis of cyberspace in the military and modern armed forces, especially in the NATO forums, has defined, for all the forces, including the naval ones, the need for strategic approaches related to the future war, a complex war that integrates and concatenates hybrid war, cyberwar, the fight against terrorism, but especially their expression and interconnection. The current technological developments and approaches embedded in the new technologies and information technology have a special impact on the security space and the battlespace. Even if, in fact, we are in a continuous war, which mainly includes the economic, financial and informational fields, it is necessary to look for and use new capabilities based on artificial intelligence – related to the computer field, which must allow the exploitation of the mega-data and determine an appropriate behaviour in the cyberspace in order to deal with them and counter them as well. We will further highlight our concerns in this regard.

Keywords: cyberspace, security concept, artificial intelligence, naval cybernetics, cyberculture.

THE CULTURE OF NAVAL CYBERSECURITY

The culture of cybersecurity is not and should not be only the specialist's concern, but of the entire staff of an organisation, either it is an economic, education or military unit etc. They all have, at this time, the intrinsic obligation to form a cybersecurity culture, because, today, such a culture is basic support of any organisation, person or human. It is equivalent to the culture of labour, because irrespective of our field of work – and even if we were only supported by social services – we need to know how to use a mobile phone, a computer, activate a cybersecurity programme, protect our personal data or data that are of major interest to us and the environment in which we live.

The culture of cybersecurity involves the creation and patrimony of a value system, and this requires time, experience, deep knowledge and, above all, capacity for creation in the cyberspace. The Romanian people, especially the young ones, have such an availability. Romanian computer scientists have already formed a brand, both in the country and abroad.

All the states of the European Union and all over the planet have started to pay special attention to cybersecurity and fight against cybercrime for several years. The cyberattacks have intensified, amplified and are well organised and coordinated. That is why both the European Union and the North Atlantic Alliance consider the protection of critical IT infrastructures against such attacks, as well as countering and combating cyber threats and threats have already become zero priorities.

Our country recognises the existence and extent of such dangers and threats and has started the concrete action, together with the NATO military partners but also with the specific structures of the EU, in a common, integrated and coordinated approach[1], in order to develop an appropriate response to this type of threat.

"Romania's cybersecurity strategy presents the major objectives, principles and directions of action for knowing, preventing and countering threats, vulnerabilities and risks to Romania's cybersecurity and for promoting national interests, values and objectives in cyberspace"[2].

[1] ***, *The Government of Romania, Decision no. 271/2013 on Approving Romania's Cybersecurity Strategy and the National Action Plan on the Implementation of the National Cybersecurity System*, available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Security StrategyCiberneticaARomaniei.pdf, retrieved on 08.09.2018.
[2] *Ibid*, p. 6.

One of the important goals set by Romania's Cyber Security Strategy is *"developing the culture of population security by raising awareness of vulnerabilities, risks and threats from the cyberspace and meeting the need of ensuring the protection of their own information systems"*[3].

This concern is universal. Nothing can stand the test of time unless it is based on a solid culture. And culture means, above all, the patrimony of certain value systems in the respective field. The computer field is relatively new, and the development of a cybersecurity culture is just beginning.

In the third quarter of 2017, Freeform Dynamics, at the request of CA Technologies, carried out the study *Integrating Security into the DNA of Your Software Lifecycle*, attended by 1279 professional IT managers worldwide, of which 466 from the European continent in six countries: Germany, Spain, France, Italy, Switzerland and the United Kingdom. The quantitative component has been completed by a substantial qualitative component, which targeted the leading professionals in the field[4].

According to the first findings of this study, companies, as a rule, do not carry out secure programmes and do not take into account their importance. The problem of cybersecurity and protection of information systems seems abstract and even non-priority in many of the units and identities studied. Cybersecurity involves a large number of restrictions, and one of them – application development and integration – is usually neglected. However, this study aims to promote a DevSecOps-like approach, which means development with native security and its skilful use in production.

However, according to this study, growth within an enterprise is favoured by the development of applications (88% of respondents), while 86% see, in this, the key to their numerical transformation. In a percentage of 79% of French and 71% of Europeans, the respondents consider that the security issue related to the development of applications is increasingly serious[5]. In a rather high percentage, of 58%, French respondents say that the main fault of this state would carry the famous *"culture of the enterprise"*, namely bad habits. It seems that, in a way, the classical culture of the enterprise, which consists of the traditional value systems, constituted in a heritage, generates a certain reluctance support to what we call

[3] *Ibid*, p. 7.

[4] *La culture cybersécurité des entreprises insuffisante, La culture cybersécurité des entreprises insuffisante le 03 Avril 2018*, available at https://www.cio-online.com/actualites/lire-la-culture-cybersecurite-des-entreprises-insuffisante-10203.html, retrieved on 09.09.2018.

[5] *Ibid.*

a cybersecurity culture, in the sense that such a culture, besides the fact that it is cumbersome and difficult to fix yet in perennial value systems, which influence the axiology and ethics of the team, did not have enough time to sit down, to be noticed and accepted as a support, as a basis that would lead to the full knowledge of the new tasks, and, on this basis of a new type of behaviour, no sufficient force to convince.

The lack of qualified personnel, as a cause for insufficient cybersecurity, was invoked by 45% of the French respondents, while 62% believe that this is only a lack of time. But 92% of the surveyed specialists consider that integrating security issues throughout the entire development process and not just punctuality is essential. However, such integration involves just highlighting cybersecurity needs, not as a fashion or as an option, but as a necessity of zero degree. However, this is not accepted, precisely because the staff has not yet formed a solid culture of this type of security, and this type of security is not yet considered an absolute necessity.

In a first analysis on this issue, the study reveals major failures in 77% of cases worldwide. Respondents are of the opinion that behavioural analysis and intelligent machines could help to compensate for the lack of time and trained personnel.

Under the current conditions, in which cyberattacks are multiplying almost exponentially, leading to increasingly diversification, greater complexity and greater sophistication of the code used, affecting a very large number of organizations, including in highly secure areas, such as the military, the formation, development and promotion of a cybersecurity culture in each unit, regardless of its profile, size and location, becomes a priority for economic and military decision-makers, and beyond[6].

However, this cannot be achieved very quickly, even though the advances of the information society, as an extremely important foundation of the knowledge-based society, are impressive. The age of cybersecurity has just begun, and some do not take it too seriously. Or even they understand that the new global, regional and national security/insecurity environment is becoming increasingly dependent on cybersecurity, there are still reasons why some managers do not concentrate their cognitive effort, much less the material effort and the financial one to face these new challenges.

There is still, among some of the managers and users of the information systems, a rather strong feeling of invulnerability, and for others one of confusion,

[6] Available at https://www.cyber-day.info/Cyberdayinfo-Instaurer-la-culture-de-la-cyber-securite-un-enjeu-majeur-pour-les-entreprises_a104.html, retrieved on 09.09.2018.

which comes from the insufficient knowledge of the field, that is due to the lack of a solid culture on this very topical theme.

At the same time, there are also managers who believe that the problem of cybersecurity belongs to IT specialists, experts in the field and even intelligence services. Therefore, this being their job, they are the ones who also need a culture of cybersecurity and the necessary skills.

In these conditions, it appears, as a direction of primordial importance, the awareness of the leaders on this issue and, especially, on the need for the emergence of a cybersecurity culture[7].

Cybersecurity is not a problem with simple solutions, within the reach of anyone, and it is not solved just by investing in equipment and software. Of course, without proper equipment and without a proper software, computer systems do not help much, and, in this case, they do not bring that expected or planned computer and cognitive value nor do they have sufficient cybersecurity guarantees.

But modern material and solid infrastructure are not enough. Managers and users matter a lot. Today, it is known that cyberattacks are increasingly complex, more frequent, more sophisticated and surprising, as they are carried out by professionals and professional organisations that innovate all the time, the action by surprise being one of the basic principles of their activity.

This is also the reason for the success of a cyberattack. Hackers are always looking for the most complicated and newest means and procedures, innovating in this field and always looking for initiatives on their immediate interest vector. Their objectives are numerous: to earn as much as possible, to weaken and even to destroy the reputation of some enterprises, personalities, anyone; to use or destroy databases, programs and projects, penetrate the extremely well-secured systems of the armed forces of great powers and even of any other country, if there is an interest in doing so, in databases and documents different services and information or security agencies, in the networks of banks and other important institutions, etc.

The idea that only technologies are vulnerable is not a very realistic one. Not the opposite. Often, users or leaders – including those with military systems and means – can form their belief that the technology they have or work on is, ab initio, invulnerable, especially when it comes to high-tech, state-of-the-art technology. And the one that equips the military means is, usually, a high-quality one, which has many complex and sophisticated security systems.

[7] *Ibid.*

Of course, such a belief is useful, in the sense that the user or operator must have great confidence in the weapon system or the means it uses. But is not enough. In the system and processuality of cybersecurity, the behaviour of the operator, the user, the system or process manager, his beliefs and the representations he makes about the security framework and the dynamics of such a national and international security environment matter very much, including cybersecurity.

CORRECT AND COMPREHENSIVE APPROACH

This behaviour is not and should not be caused by mere impressions or what others say. It must have, on the one hand, an extremely strong cybersecurity culture, based on heritage values, even if this heritage is very young and still quite thin, on the experience accumulated over time, and, on the other hand, on the principles of sufficient reason and methodical doubt, whereby the situation of cyberspace reports and actions is subject to logical reasoning and necessary questions.

The logical, coherent, careful and prudent behaviour, as well as the courage based on the thorough knowledge of the support of the action are both extremely important elements of effective human action in any field – and even more so in cybersecurity, a very special field –, as well as vector expressions of a cybersecurity culture.

Organisations that promote such a culture among staff are much more capable than others of defending against cyberattacks. Because the staff knows what it is about, has what it relates to, knows what has to be defended and always acts knowingly.

Cyberrisk cannot be fully known or prevented. Of course, it can be assessed according to the degree of knowledge of cyber threats and the vulnerabilities of systems and processes, means and actions of any kind to them. That is why the cybersecurity specialist within any organisation, including the group responsible for the maritime operation, at the TG level, the management systems and even within the battleship – the basic unit of the Naval Force – must have himself a very solid cybersecurity culture.

This specialist is not and should not be just a simple user and user of algorithms and programs for securing computers, servers and networks, but one with an equally technical, operational and even strategic vision, able to know, to understand and coordinate the full range of activities involved in the cybersecurity of a domain. Because, in our age, such security is part of a war without limits and without theatres of tangible and manageable operations – the cyberwar. This specialist must be able

to understand and put into operation the description of the operational field, the cyber IPB characterised by the strategic requirement, operational and even tactical procedures, materialised by the characteristics of the cyberattacks carried out in the area of operation by the adversary and connect the past actions both successfully completed but also those missed.

The cyber domain revolutionises and, at the same time, upsets the rules, not only the ordinary ones but also those in the codified and secreted world. It upsets and revolutionizes them extremely, as it introduces new and new dangers and threats into and through this constantly identifiable and constantly expanding numerical space. These threats concern not only banks, governments, companies, big concerns, in the end, the economy, information and finance services, transport and telecommunications, but also all the components of the armed forces, especially the high-tech ones.

For example, the French armed forces are one of the modern armed forces of the world. It is on the 5th place among the first 10 armed forces of the Earth, with 385,635 professional military personnel, 1,305 aircraft, 406 tanks, 118 warships, 4 aircraft carriers and 300 nuclear resources, which means exceptional military, technical and informational training and high awareness of its role in defending France and maintaining the balance of military power in this increasingly tense, uncertain and dangerous world.

These armed forces, like any other modern armed forces on the globe, are facing a new challenge of cyberspace war. This new type of war changes the panoply of the god Mars substantially. So far, in any type of war, including high-tech and network-based warfare, asymmetrical, asymmetrical, hybrid and even unlimited warfare, which is increasingly being talked about, the enemy was identified, and the confrontation was identified. it took place in a physical space – land, sea and air – in which manoeuvres of all kinds were used, which made it more ingenious, sophisticated and surprising. Today, when warfare tends to be robotic and extended into cyberspace, the military is required to change both strategies and mentality, means and, especially, languages, in order to always be able to identify, understand, to know and describe the new types of challenges, dangers and threats (we refer in particular to those generated by cyberspace or which are manifested in what we call cyberspace).

In this regard, the commander of the cyberdefense within the French General Staff showed that *"digital threatens all soldiers, even at home"* – a fact that is true and unanimously valid. In the same extent, he noticed the multiplication

of the attacks on the psychological balance and the emotional stability, through negative and scary messages that broadcast twice faster than the ones known so far. It follows that the information disseminated itself becomes not just a weapon, but a new and very special battlefield.

To cope with this new type of war, stresses the author, the French armed forces feel the need to expand their network, especially through diplomacy and cooperation. In their old pride and dignity, they were accustomed to budgetary constraints and resilience, which forced them to keep their equipment and procedures as long as possible. According to the new imperatives, information arrives very quickly in security deposits, but not to be preserved, but to be integrated into a whole, as integration and integrity are, in the new era, the only viable medium on which a response can be developed. tailor-made to such a new, dynamic, fluid and very complex type of challenge.

This is neither simple nor sufficient. Therefore, according to the author of this point of view, the French armed forces must adopt innovative strategies and actions, restructure its ecosystem, thus integrating their personnel and processes into a new concept, in order to generate that favourable framework for cybersecurity integration. in a short cycle.

In order to manage the reaction to an unidentifiable threat, the French Armed Forces have set up an innovation agency, which brings together the research with the operational side, thus contributing to the integration of industries in a continuous development trend in a new conceptual defence horizon, based precisely on the extremely fluid and complicated dynamics of cyberspace.

Today, adopting a strategy is not a simple thing. Beyond the fact that you need to identify and know all the challenges, dangers and threats and their dynamics in time, space and concepts, you must work with the allies, take into account the dynamics of the space of the fight, the real possibilities of the forces, the means, the resources and conjunctions. Of course, all this is well known to all the armies in the world, because that was and still is their mission.

But today things are changing because of this cyberspace. In today's world, the United States is the first cyber target for cyber pirates coming from the East, the Middle East and even the Far East. But they often forget to say, the author points out, that the US services are the first cyber spy on the planet, even spying on their allies, and that France continues to pay terrorism a living tribute in human lives. Despite this finding, which does not seem to be all right and reminds us of France's unique position at different times in NATO history, France's cyber defence

commander launches an astonishing one: However, we must help our American friends!

The same thing happens with those who develop cybersecurity solutions. It is difficult to get along with them, and military officials consider it a real pain to comply with what they ask. The armed forces must comply, however, with the new situations created by the digital transformations of the state, but they are expected to use systems on which to have sovereignty, which, of course, is very difficult.

In 2017, cyberattacks cost French companies, which were victims, 550 million euros. The French gendarmerie was closer to these companies and, therefore, is more pragmatic in understanding this situation than the whole French armed forces. The person in charge of the missions in this digital field of the French Gendarmerie speaks about the network of innovators in France, paying special attention not to the innovation of the force, but rather to the developers. The cyber domain requires those responsible to move faster, to find solutions so that they can have a response from the police perspective, to assemble testimonies to understand and respond to the threat. Hence the need for a network to retrieve incident information and respond promptly.

It remains that, in order to respond to threats of this kind, the French Armed Forces must acquire and respect a series of experiences and practices already faced by companies in this country.

The constraints and resilience of the armed forces are much stronger than those of businesses and administration. Therefore, there is a need for increased capacity to use their own networks, even if they are degraded. However, in the vision of the French cyberdefense commander, he must have the ability to always stand up, to deploy communications systems quickly.

In order to remain one of the pillars the importance of the state's response, the armed forces, although faced with the lack of specialists in this field, have to look for people competent in the fields of artificial intelligence (AI), data analysis and scientists. Hence the need to reorient the training system in this institution.

In other words, training for the military in any military service must also include a cybersecurity component, not as a voluntary annex, but as an integrated component in each of the other components, all together. forming a unitary whole. Cybersecurity management – a novelty in the matter of preparing the armed forces – although it is a special type, must be integrated into its overall training.

This approach takes into account, on the one hand, a specific ideology of this type of integrated management and, on the other, on the extension of the military

culture – strategic, operational and tactical – with a component that, although it will exist almost in itself, it will, in time, as we shall also demonstrate in this paper, become one of the pillars of resistance and force in the preparation and operation of the armed forces and all their services and means, including naval ones.

CONCLUSIONS

Cybersecurity has emerged as an objective necessity, but not for securing cyberspace (because cyberspace is merely a virtual ocean, an action-support theatre, a vector theatre, and not a recognisable and manageable entity or identity), but for their own security, mainly by means of computer systems, by cyber means.

The cybersecurity of a naval platform must be managed and addressed continuously, with sufficient expertise for the complex coexisting environment, but also flexible, in accordance with the cybersecurity of all related components of the theatre of operations, imaginative, unidirectional and adaptable continuously and constantly. in any situation, but especially they can overcome and predict.

Cybersecurity is only a component of security among others, it is not integrated, by the network, complexes and definers, and their configuration, planning, assuming and assuring are legal of cyber vitality of all platform environments and not only, of continuous cooperation, by the action and the rapid action, proportionate for all the systems, in conditions of multiplication of the unpredictable variables and a risk of liquid.

HUMAN RESOURCE
– THE MOST IMPORTANT COMPONENT OF COMBAT CAPABILITY OF ARMED FORCES –

Mihail ORZEAȚĂ, PhD
Professor, "Apollonia" University, Iași

The main objective of human resource training in any armed force should be mentality and attitude change from the reactive one to a proactive and winning mentality. Military profession is honourable but very demanding as well because it entails a high degree of risk and devotion up to sacrifice. The current number of the Romanian Armed Forces' military personnel is smaller than the one before 1989. That is why they have to be better trained than their predecessors to accomplish assigned missions. NATO is the organisation that imposes professionalism, responsibility, legality and team spirit to all its members including Romania. The military leader must be the role model for all his/her subordinates, knowing how to lead them and his/her military unit in order to accomplish any assigned mission.

There is no need to tell a well-trained military person twice WHAT to do to.

Keywords: mentality, attitude, leadership, permanent change, professionalism.

INTRODUCTION

Human resource had and it will continue to have a very important role for building the Armed Forces combat capability. As a consequence, military leaders have to identify adequate solutions for training the human resource in a way that will increase the combat capacity of the Armed Forces up to the maximum value.

Napoleon once said that *"any private carries a field-marshal's baton in his knapsack"*[1], referring to promotion and to increase competence and professionalism as well. In order to accomplish this objective any military person has to make continuous physical and psychological efforts. For the same reason society has to allocate financial, material and technical resources.

The Armed Forces that hire well trained militaries and possess performant weapon systems will be credible and will sustain national defence and security strategy as well. Moreover, such Armed Forces will contribute to the society protection from any type of risks and threats and, if necessary, from any external aggression.

MENTALITY AND CONTINUOUS LEARNING ROLE IN MILITARY PERSONNEL TRAINING

Mentality has a decisive role in human performance

Many politicians and military analysts, experts in international relations, futurists, economists, computer scientists, sociologists and so on have written and will write studies about information age, globalisation, changing world and transformation. Continuing debate on the above-mentioned topics is necessary because information explosion and globalisation oblige us *"to redefine our existence coordinates"*[2]. Otherwise, *"if we stay and do nothing the shock will be so rapid and will have such a magnitude that we will not be able to deal with it"*[3].

Therefore, we have to acknowledge that *"the only constant of today's world is change"*[4] and also that continuous change is the only way to adapt ourselves

[1] Dictionary of Quotations, *Napoleon Bonaparte*, see https://www.bartleby.com/345/authors/352.html, retrieved on 10.08.2019.
[2] John L. Peterson, *The Road to 2025*, White Group Press, Corte Madera, California, 1994, p. 340.
[3] *Ibidem*.
[4] John Huey, *The New Post-Heroic Leadership*, in *Leadership in the 21st Century*, Air University Press, Maxwell Air Force Base, Alabama, USA, 1997, p. 3.

to the international environment evolution in order to maintain viable Armed Forces from conceptual, structural-organisational and operational points of view. This way of thinking and acting entails a proactive and winning mentality which will help us to overcome reluctance, convenience and fear when we have to adapt to the international environment. The achievement of winning mentality is possible only when we will focus on militaries' adequate training because they have an important role in any human activity, at individual and collective level as well, considering the employed measures and performed actions.

Continuous learning – certain way for achieving performance and professionalism

The existing studies conducted by notorious scientific researchers show that *"approximately 80% of developed countries' welfare was obtained through the human capital contribution"*[5]. Moreover, many famous experts state that the future belongs to the *"knowledge society"*[6] as well as to continuous learning. Therefore, in order to achieve performance and efficiency, military education and training have to implement mental adaptation to permanent change, in connection to future's requirements.

Our society evolution as well as its military organisation depends on the international environment. Globalisation and information entail some *risks, vulnerabilities and threats* to individual, national and international security. In order to avoid *risks, vulnerabilities and threats* it is necessary to estimate international relations system tendencies and to envision how to develop the society and its Armed Forces in accordance with these tendencies. The achievement of this objective depends on people's quality because they have to permanently fight with themselves against obsolete mentality as well as convenience, against all kinds of fear, weakness and failure.

The international security environment evolution compels us to take decisions today that may have effects in the future. As a consequence, we always have to be very well informed, to permanently analyse the trends in the internal and international environment we live and work in, and to look for solutions to harmonise these trends with our plans and programmes for future developments. Moreover, in this respect, we need to know very well our capabilities because this is the right way to identify solutions and to adopt decisions according to political, economic,

[5] Roger Ibbotson and Gary Brinson, *Investment Markets*, McGraw-Hill, New York, 1987, pp. 21-25.

[6] Academician Mihai Drăgănescu, *Societatea informațională* şi *a cunoaşterii. Vectorii societăţii cunoaşterii*, Academia Română, p. 26, see https://documente.net/document/mihai-draganescu-societatea-informationala-si-a-cunoasterii.html, retrieved on 22.08.2019.

financial, social, cultural, military and ecological environment's requirements. This way of thinking and acting means to accept, implement and acknowledge continuous learning in our lifestyle. This concept is characterised by initiative spirit, which, associated with an adequate capability to estimate and inform, will allow us to avoid undesired events, more precisely, to be aware of what may happen and to take the appropriate measures to adapt ourselves to any situation.

First of all, continuous learning means to very well know ourselves. Any major change has to be carefully prepared. Mentality change is a laborious and long process. That is why the first step in achieving this objective must be *self-knowledge*[7], which needs to permanently be accompanied by self-assessment and self-improvement. Every military person must know his/her psychological and physical limits and have the impulse to push these limits forward through *continuous learning* and to adapt himself/herself to always more demanding profession requirements.

Continuous learning is the right solution to reach performance and become outstanding military professionals. This concept entails that education within the institutionalised system should be followed by studying independently as well as by learning all the lessons from training activities and from real missions performed in theatres of operations.

Continuous learning also means *to be efficient* in everything we do. That is to say *to have respect for time*. Although time is implacably flowing, it does not mean that it is our enemy. We need to better understand how to use the time in order to be our ally or at least not to be our adversary. History lessons tell us that, more often than not, success in economic, political, financial and military competitions/confrontations was achieved by capitalising on surprise[8], and that surprise comes mainly because of different perception of time factor. The most probable type of surprise during military actions is the one in which we do not timely know the adversary (enemy) intentions and our available time till the beginning of the action is not long enough to take appropriate measures to appropriately prevent or counter them[9]. In fact, this kind of surprise is generated by the *reactive mentality* which is based on post-factum action that gives little freedom of initiative to people

[7] Camelia Jianu, *Rolul autocunoaşterii* în *dezvoltarea personală* şi *profesională*, Asociaţia Profesorilor din România, 08.02.2012, see http://www.asociatia-profesorilor.ro/rolul-autocunoasterii-in-dezvoltarea-personala-si-profesionala.html, retrieved on 02.08.2019.

[8] William McLaughlin, *The Element of Surprise – Totally Effective Surprise Attacks in Military History*, War History Online, see https://www.warhistory.online.com/world-war-ii/the-invasion-of-crete-last-m.html, retrieved on 12.08.2019.

[9] Mark F. Cancian, *Coping with Surprise in Great Power Conflicts*, Center for Strategic International Studies (CSIS), February 2018, p. VIII, see https://csis-prod.s3.amazon.aws.com/s3fs-public/publication/180227_Cancian_CopingWithSurprise_wAppen_Web.pdf , retrieved on 14.08.2019.

who have it. A reactive mentality is another way of saying that *we are living in another time frame than the one we live in*.

Continuous learning implies also to reject attitudes like *"it is fine too"* or *"a wonder lasts for only three days"* and so on. The inadequate use of available time because of the military personnel mentality and misorientation towards performance may cause missing opportunities, creating dysfunctions in achieving the synergy of all the components that generate the Armed Forces combat capability. This situation could be the cause of our country reducing or even losing credibility within the Euro-Atlantic organisations – NATO and EU – Romania is part of.

To be efficient means to timely accomplish all the missions and consume as less as possible resources. People who disrespect time get used to saying that *"time solves everything"*. An efficient human being must know HOW and WHEN time solves what he/she should solve by himself/herself. The world for which every military person must be prepared is first made for those people that have no fear for the new, for those that fight for being performant in everything they do, for those that do not give up when they face the first serious obstacle while conducting actions to accomplish an objective (mission). Gaining success in the military confrontations of the 21st century may not belong to people that act guided mainly by routine, to those that are less adaptable and less professional from the military point of view.

In a world of permanent change some today's certainties may become history tomorrow, and uncertainties (in a probabilistic meaning, that is to say there are not constant data but medium probabilistic values) will be more and more part of our life. In this context, uncertainty needs to be understood as a point of reference in a process that evolves, so it is as it is for some time, then it has to be updated, reassessed, resized and so on). Such perspective may scare a less informed person but even the one that is not accustomed to take decisions which will have important effects months or even years after that. Moreover, a person might be scared if he/she is not so comfortable to permanently fight against time as well as against an environment dominated by permanent change (transformation, evolution).

It is possible to eliminate fear of such a future by motivating every people to contribute to shaping the future in accordance with his/her proved possibilities. The efficient actions of any type of organisation/institution depend on the active, responsible and adequate participation of all framed categories of personnel while the weakness of any team (structural entity) is given by its *"weak link"* – that is to say the person that is incompetent for the position filled within the organisation/institution.

INVESTMENT IN PEOPLE AND PERMANENT SELECTION – COMPULSORY STEPS IN GAINING COMPETENCE AND IMPLEMENTING A NEW STYLE OF INSTRUCTION AND LIFE WITHIN THE ARMED FORCES

Investment in people – sine qua non condition of success

People have been the most important resource of every community throughout history. This is true today and it will be true as long as humans will live on our planet because people generate ideas and they will set up plans and programmes to utilise the existent potential of the society in order to make ideas, visions and objectives come true.

Human resource is the essential component of any human activity because it is the leading factor of the process as well as the one that controls and implement plans as well as programmes. Moreover, the human resource assesses the results of the process and takes the appropriate measures to adapt plans, programmes and, if necessary, even objectives and directions of actions in order to meet the changes of a new context of activity within the environment.

There still exist some dysfunctions within the process, especially in terms of the personnel information and accountability. Some people complain that they do not know how their future looks like and what it is there for them. It is hard to understand this attitude, considering the existing *strategies* – at national, department, sector, and other levels –, which are the basis for building plans and programmes to be implemented for all the structural entities of the military organisation. In my view, the simplest solution to make all the military organisation personnel acknowledge and become accountable is to *permanently and consistently invest in people.* However, it is not that simple to implement it.

The human being differs from all other beings that live on this planet due to the ability to think. As a consequence, the key for every human action is located into our minds. Therefore, any step of the process meant to increase the Armed Forces combat capability has to begin with the personnel. The most important stages of this process should be: education, training, skills formation and development, as well as people motivation. Collin Powell said that *"ideas can rise and ruin empires"*[10], whilst we know that the idea is just the beginning of any process. In a similar spirit, an author well known for his books on success philosophy believes that *"no man is defeated unless he abandons fighting, in his mind...* [because – A.N.] *human mind builds or ruins ...* [because – A.N.] *our only limitations are those we set up in our minds"*[11].

[10] Oren Harari, *Secretele lui Colin Powell*, Editura Tritonic, București, 2006, p. 40.
[11] Napoleon Hill, *De la idee la bani*, Editura Curtea Veche, București, 2008, pp. 39, 118, 137, 270.

The right military persons into the right positions through permanent selection

Many times, people know WHAT they have to do but they do not know HOW to do it or they are afraid to apply their knowledge. Although it has often been demonstrated that fear is the most inappropriate counsellor, because it paralyses initiative, some military persons need more support, tutelage or one more approval from their commanders/managers for doing what they have to do in compliance with their job description. Such attitude will most probably generate failure or, in the best case, dysfunctions that entail higher than planned resource consumption for correcting the course of action as well as less efficient results of the programmes that may negatively affect the whole process of increasing the Armed Forces combat capability.

Life was and most probable will be a continuous fight[12]. At the beginning of his existence the human being was obliged to fight for survival with the Nature and with other humans. Currently, the most important fight of the humans is the one for progress by reaching new peaks of knowledge and transforming them into strategies, concepts, algorithms, procedures, tools, technologies, devices, works of art, new substances and so on that should help us to have a better and longer life. In my view, fight for progress is the responsibility of every military person and it has to start against own weaknesses, conveniences and temptations, because performance requires sacrifices.

The Holy Bible says that God made man in His own likeness and gave him the task *"to rule over the fish of the sea and the birds of the air, over the livestock, and over the earth itself and every creature that crawls upon it"*[13]. Thus, the modern human is the result of permanent integration of the initial gift of the Creator into the accumulations of all the following generations that lived on the planet Earth. Therefore, we, the humans, are not only a product of divine creation but also of own will. However, each of us are what we want to be if we have a strong will because the *"individual will influence the progress of mankind"*[14]. A strong will is not enough to accomplish all our objectives, especially when they are not realistic, that is to say the objectives are not correlated with our capabilities. That is why the necessary and sufficient conditions for success are: *to want but also to be able to do* what we want.

This is the reason why the investment in people should be accompanied by the permanent selection of the human resource in order to motivate (encourage,

[12] George Coşbuc, *Lupta vieţii*, see https://www.versuri.ro/versuri/george-cosbuc-lupta-vietii_t217.html , retrieved on 10.08.2019.

[13] *The Bible, Genesis, 26*, Gute Botschaft Verlag 1989, 1990, Dillenburg, West Germany, p. 2.

[14] Marcus Mabry, *Condoleezza Rice şi drumul ei către putere*, Editura Curtea Veche, Bucureşti, 2008, p. 133.

promote) those that want and can be performant and role model. I am referring to those people who, after a period of education and training into an institutionalised system, are able to continue their personal development[15] using continuous learning. This personal evolution should be based on their professional competencies and gained experience for fulfilling the established objectives and creating or having an active participation in the development of new strategies, doctrines, concepts, plans, programmes and so on, aiming to contribute to setting up a more performant military organisation.

The permanent selection of military personnel should help them to discover their abilities and to find the positions within the Armed Forces that are the most suitable for them, in accordance with their potential and performance.

The objective of investing in people and, implicitly, of permanent selection should be *to find the right military persons for the right jobs/positions* within the Armed Forces.

Implementation of a new training process and of a new life style in accordance with 21st century requirements

Information explosion is no longer a fashionable phrase but a reality that dominates our daily existence.

The need for permanent change must be acknowledged in order to cope with the 21st century requirements and to manage to adapt ourselves to contemporary political-military phenomenon's tendencies as well as to implement a new method for *training and living*.

The training process and the life style I am referring to entail transforming the prevalent reactive mentality and attitude into a proactive attitude accompanied by a winning mentality. In order to have this objective fulfilled it is not necessary to wait until an event happens and then to act. Usually, post-factum actions are meant to repair damages or to limit the undesired effects, so they are not recommendable.

Changes occur at a high speed at global level and this speed may surprise everyone and generate *resistance, opposition* or even *inadequacy feeling* at the level of the individual or a group of people (military entity). The avoidance of such situations is possible by adequate training and participation in order to provide each military person with the opportunity to mentally connect to this objective.

This kind of training process is compulsory for eliminating psychological barriers and the resistance to new ways of thinking and acting. As the knowledge limits

[15] Stanley J. Gross, Ed. D., *How to Raise Your Self Esteem*, PsyhCentral, see http://psych.central.com/lib/how-to-raise-your-self-esteem/000737, retrieved on 04.08.2019.

extend it is possible for some today's truths not to be truths of tomorrow or to be only partial truths. In the past some people were burned alive if they advocated ideas that were considered heresies[16]. Currently, new ideas are welcomed if they result in progress and improve our life.

In order to avoid the risks and threats to individual, national and international security, which cover a large spectrum, from conventional to unconventional and terrorist attacks, it is necessary to know the situation in the international security system in real time, to estimate its evolution and to take timely measures for preventing or adapting ourselves as well as our institutions. The adaptation I am referring to differs from the lack of firmness and stability. Firmness is necessary to achieve objectives not to maintain *obsolete ways of thinking and acting to fulfil them.* The mentioned ways can change, depending on the available resources, means, time and other factors that describe the context of action.

This way of thinking means flexibility in decision-making and acting to allow the system to keep its viability no matter the situation. Thus, any change in the environment (risks, threats, own capabilities, priority redefinitions and so on) should be carefully analysed to assess the possible ways of influencing the process (action) in progress, ways that need to be disseminated to all the system's elements, which can be affected in a way or another.

Keeping the viability of the military organisation in a permanently changing world compels us to learn how to develop concepts, plans and programmes based mainly on variable data (medium probabilistic values that describe the prognosis of the events' evolution and the environment analysed factors), because initial data may change anytime and it will be necessary to restart, partially or integrally, the planning and analysis process. In other words, *"the best way to predict future is to <invent> it"*[17].

In today world the war is won mainly because of mental superiority[18] characterised by proactive attitude, capability of prognosis, synthesis and decision-making. Moreover, to win the war means to appropriately employ the available potential: human resource, weapon systems, finances, real time collecting, processing and disseminating information, decision-making cycle, which has to be shorter than the adversary's, permanently outrunning the adversary's actions, and so on. This is the world where there is no place for non-professional, hardly adaptable, routine people, as well as for the ones that fear of new ways of thinking

[16] Giordano Bruno was burned alive as heretic by the Jesuits because he said that the Earth revolves around the Sun and not vice-versa as it was stated (known) at that time (*Giordano Bruno*, Scientia.ro, 06.04.2010, see https://www.scientia.ro/biografii/41-biografii-fizica/776-giordano-bruno.html, retrieved on 02.08.2019).

[17] T. Nelan, L. Goldstein, J. W. Pfeiffer, *Plan or Die*, Pfeiffer & Company, San Diego, California, 1993, p. 76.

[18] G. T. Hammond, *The Essential Boyd*, Air University Press, Maxwell Air Force Base, Alabama, USA, 1997, p. 6.

and acting. The elimination of the fear of the future is possible through motivating people[19].

That is to say power comes from within us, from our will to fight for overcoming our limits, to fight for proving the correctness of our opinions and solutions and not accepting less competitive ones. Military persons should understand that winning a real armed confrontation is possible through the integration of all the capabilities of the nation within the effort required by the confrontation environment. The current and especially the future armed confrontation encompasses multiple domains – politics, diplomacy, economy, finances, psychology, culture and military, more often than not simultaneously. This reality requires multidisciplinary and continuous training.

Future armed confrontations will be multidimensional and integrated. That is why military persons must be very well trained in any dimension of the armed confrontation to withstand and win, not only in the physical battlefield but also in the mental one.

In peacetime states are engaged into different competitions – for resources, influence, territories and so on – and some of them will not hesitate to use any means for winning the competitions they are part of. This way of doing business is well described by an American writer who states that we live in *"a world in which those who do not hit with their legs, do not deceive, do not grab things in a greedy way, and do not do all these things with a certain style and grace, will remain to pay the bill while the winners go to the next club in fashion"*[20].

CONCLUSIONS

Having a *proactive mentality* means anticipating the events and taking preventing measures to avoid undesired events. This way the *winning mentality* is highlighted, in relation to the proactive attitude, the initiative spirit and the desire for success, based on competence, adaptive capacity to different contexts and courage to assume responsibility.

It is important to learn and keep from the past only the useful and valuable things and ideas, and to build the future investing in people.

During any armed confrontation people can transform a fight that looks lost into a victory using their professional and psychological training. Moreover, fighters that are not well trained and lose their morale may lose a potential victory.

[19] Wes Roberts, PhD, *Victory Secrets of Attila the Hun*, Doubleday Press, New York, 1993, p. 18.

[20] Stanley Bing, *Sun Tzu era un biet mototol*, Editura Curtea Veche, București, 2004, p. 14.

Morale is the power's component that can bring victory in any type of confrontation[21]. Morale cannot be quantified yet although many people try[22].

Military people can engage in any armed confrontation having fear or trust in their own forces. If they want to win victory in any type of fight, military persons should neither over- nor under-estimate their adversaries.

Pope John Paul II used to say that people are like wine *"as long they get old, they may become champagne or they can transform in vinegar"*[23]. Consequently, we have to choose between the two extremes using permanent selection at all the hierarchical levels and during all the activities.

All military people have to understand that *the following fight is the most important*, and that is why the military leaders must establish the standards that need to be fulfilled, being the first to respect and achieve them. This is the way leaders contribute by example to enhancing subordinates' morale.

One of the most important military leaders' responsibilities is to motivate subordinates and facilitate the promotion of the worthy ones. To do it, military leaders must know their subordinates very well in order to use their potential at maximum and to gain efficiency by assigning them to the positions where they give maximum results.

Military leaders were and will continue to be the elite of every society. As it is well known the *"elites play a decisive role in history"*[24], but the future of all the military persons depends on acknowledging and achieving the right skills to choose between: becoming and being, contributing and receiving, transforming and maintaining the status quo.

BIBLIOGRAPHY

1. ***, Army Field Manual, Land Operations, Land Warfare Development Centre, *Army Doctrine Publication AC 71940*, Warminster, Wiltshire, United Kingdom, 31 March 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual_AFM_A5_Master_ADP_Interactive_Gov_Web.pdf
2. ***, *Bible or Holy Scripture, Genesis, 26*, Gute Botschaft Verlag 1989, 1990, Dillenburg, West Germany.

[21] William Petersen, *Von Clausewitz on War: Six Lessons for the Modern Strategist*, Columbia Business School, 12.02.2016, see https://www8.gsb.columbia.edu/articles/ideas-work/von-clausewitz-war-six-lessons-modern-strategist, retrieved on 24.08.2019.

[22] *Army Field Manual, Land Operations,* Land Warfare Development Centre, Army Doctrine Publication AC 71940, Warminster, Wiltshire, United Kingdom, 31 March 2017, pp. 3-12, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual_AFM_A5_Master_ADP_Interactive_Gov_Web.pdf, retrieved on 25.08.2019.

[23] *John Paul II*, Citatepedia.ro, http://www.citatepedia.ro/index.php?id=2685, retrieved on 10.08. 2019

[24] Ezra Suleiman, Henri Mendras, *Recrutarea elitelor în Europa*, Editura Amarcord, Timişoara, 2001, p. 291.

3. ***, *John Paul II*, Citatepedia.ro, http://www.citatepedia.ro/index.php?id=2685.
4. Stanley Bing, *Sun Tzu era un biet mototol*, Editura Curtea Veche, București, 2004.
5. Napoleon Bonaparte, *Citate celebre*, https://cuvinte.celebre.ro/si-tu-poti/.
6. Giordano Bruno, *Scientia.ro*, 06.04.2010, https://www.scientia.ro/biografii/41-biografii-fizica/776-giordano-bruno.html .
7. Mark F. Cancian, *Coping with Surprise in Great Power Conflicts*, Center for Strategic International Studies (CSIS), February 2018, p. VIII, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180227_Cancian_CopingWithSurprise_wAppen_Web.pdf
8. George Coşbuc, *Lupta vieţii*, https://www.versuri.ro/versuri/george-cosbuc-lupta-vietii_t217.html
9. Academician Mihai Drăgănescu, *Societatea informaţională şi a cunoaşterii. Vectorii societăţii cunoaşterii*, Academia Română, https://documente.net/document/mihai-draganescu-societatea-informationala-si-a-cunoasterii.html
10. Stanley J. Gross, Ed. D., *How to Raise Your Self Esteem*, PsyhCentral, http://psych.central.com/lib/how-to-raise-your-self-esteem/000737.
11. G. T. Hammond, *The Essential Boyd*, Air University Press, Maxwell Air Force Base, Alabama, USA, 1997.
12. Oren Harari, *Secretele lui Colin Powell*, Editura Tritonic, Bucureşti, 2006.
13. Napoleon Hill, *De la idee la bani*, Editura Curtea Veche, Bucureşti, 2008.
14. John Huey, *The New Post-Heroic Leadership*, in *Leadership in the 21st Century*, Air University Press, Maxwell Air Force Base, Alabama, USA, 1997.
15. Roger Ibbotson, Gary Brinson, *Investment Markets*, McGraw-Hill, New York, 1987.
16. Camelia Jianu, *Rolul autocunoaşterii în dezvoltarea personală şi profesională*, Asociaţia Profesorilor din România, 08.02.2012, http://www.asociatia-profesorilor.ro/rolul-autocunoasterii-in-dezvoltarea-personala-si-profesionala.html .
17. William McLaughlin, *The Element of Surprise – Totally Effective Surprise Attacks in Military History*, War History Online, 27 August 2017, https://www.warhistory.online.com/world-war-ii/the-invasion-of-crete-last-m.html
18. Marcus Mabry, *Condoleezza Rice şi drumul ei către putere*, Editura Curtea Veche, Bucureşti, 2008.
19. T. Nelan, L. Goldstein, J. W. Pfeiffer, *Plan or Die*, Pfeiffer & Company, San Diego, California, 1993.
20. John L. Peterson, *The Road to 2025*, White Group Press, Corte Madera, California, 1994.
21. William Petersen, *Von Clausewitz on War: Six Lessons for the Modern Strategist*, Columbia Business School, 12 February 2016, https://www8.gsb.columbia.edu/articles/ideas-work/von-clausewitz-war-six-lessons-modern-strategist .
22. Wes Roberts, *Victory Secrets of Attila the Hun*, Doubleday Press, New York, 1993.
23. Ezra Suleiman, Henri Mendras, *Recrutarea elitelor în Europa*, Editura Amarcord, Timişoara, 2001.

THE NEED FOR AN INTERNAL MANAGEMENT CONTROL APPLICATION FOR MILITARY ORGANISATIONS

Carmen Maria IEPURE (MOISE)
PhD Candidate, "Carol I" National Defence University, Bucharest
Elena CLENCI
PhD Candidate, "Carol I" National Defence University, Bucharest
Toma PLEŞANU, PhD
Professor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

The article presents the results of the doctoral research, the need for the development and use of a dedicated computer application or the adaptation of an existing one, in order to be able to track the flow of documents of the internal management control system and to connect all the planning documents, the specific objectives, the risks, the sensitive/exposed functions to corruption.

Keywords: military organisation, internal management control, application, communications and information.

INTRODUCTION

Following the doctoral research carried out, as well as the direct observations made by us, we find that it is imperative to create and use a specialized software, a dedicated application or to adapt an existing one, through which the flow of documents of the internal management control system (SCIM) can be followed and all planning documents, specific objectives, risks, sensitive/exposed functions to corruption can be connected; it will grant different editing/consulting rights, it can only be fully accessed by the deputy and the commander/chief/director of the structure and the secretariat of the monitoring committee.

Each member of the commission will be able to view the documents subject to approval, monitoring the risks associated with the objectives set, the procedural activities and the procedures associated with them.

The need for an application also comes from the finding of diminishing human resources and overloading with tasks, especially in small and medium-sized units. Also, as we can see with a single click on google.ro, there are already built applications for SCIM. However, we want a useful application for the military organization, which inherently leads us to create an application with needs adapted to the system.

Another argument that drives us to build a model for a future application is the fact that we are contemporary with the era in which information must flow quickly and efficiently so that decisions made by structure managers can be made in a timely manner, based on complete, accurate and real-time information. Access to quality and real-time information makes the difference between a right decision and a wrong one.

It has become an organic necessity to build applications that will streamline the flow of data and information, in the context of maintaining a managerial performance as adapted to the century in which we live.

Another essential aspect in the decision to propose a computer application is the ease of continuous monitoring at the organization level. Permanently, the people who access the application can complete, with existing data and information, the documents existing within it.

Data processing by computer software is faster, thus avoiding a lot of dead times, which, in this century really matters. Computer applications add value to institutions, whether they are state or private, because information that is useful

to the process of running the organization can be much easier to obtain. This type of data access is known in the American literature as a management information system (MIS)[1].

These systems, designed for organizations, can incorporate different performance functions that can guarantee a superior decision-making process. Through them, a large number of reports and situations can be issued that can be generated automatically only by entering some primary data.

The United States of America has been the promoter of these types of systems since the 1960s.

There are several management systems developed by large software companies. Of these, we list:

- SQL Server 2005 with Analysis Services;
- Office XP / 2003;
- Data Analyzer;
- MapPoint;
- SharePoint Portal Server;
- Project Server 2003;
- Microsoft® SQL Server ™ Accelerator for Business Intelligence.

A schematic description of this concept is described by Dr Sourabh Sharma & Professor K.S. Thaker[2], as shown in the figure below.

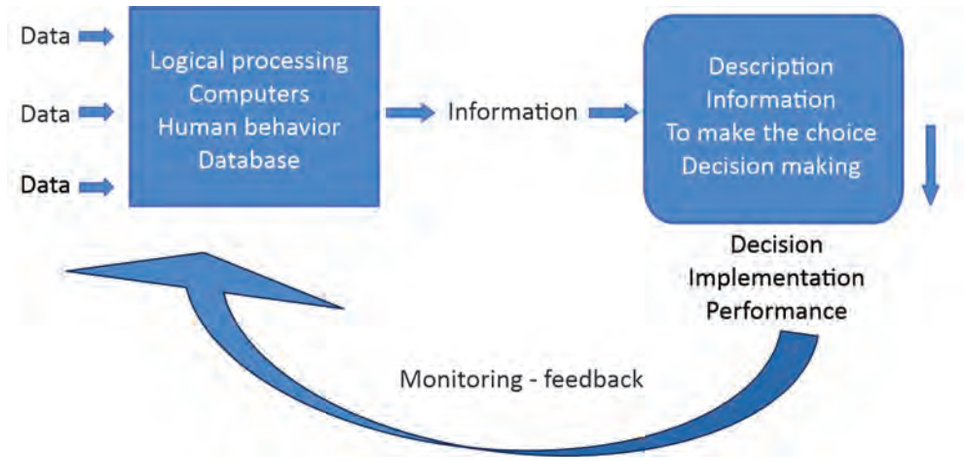


Figure no. 1: Management Information System (MIS) concept

Source: adaptation by *Dr Sourabh Sharma & Professor K.S. Thaker, Management Information System, Horizon Books, 2015*.

[1] See https://www.shopify.com/encyclopedia/management-information-systems-mis, retrieved on 04.04.2019.

[2] Dr. Sourabh Sharma & Prof. K.S. Thaker, *Management Information System*, Horizon Books, 2015.

This schematic description of the MIS concept presents, through a simple diagram, the processes that must be carried out within an organization with an efficient management. In order to be successful every organization needs strong leadership and commitment from top management to support a successful strategy.

ADVANTAGES AND DISADVANTAGES OF USING A COMPUTER APPLICATION

In the following we will present five of the most important advantages and disadvantages of using a computer application, from our point of view. They are:

Benefits	*Disadvantages*
Easy management of information	Risk of theft or data loss
Provides detailed information and reports that can be used for complex analysis, identifying opportunities for improvement and developing strategies	Costs for development, implementation, licensing, maintenance, upgrades, staff training
Increasing the efficiency of operators	Dependence on a network
Access to information in real time	Dependence on a supplier
Accuracy and standardization of data	Difficulties in using the application due to the complexity or lack of training

❖ ***The advantages of using a computer application*** are as follows:

The first of the advantages, in our opinion, is the easy management of information, which means ensuring a real forecast and a proactive approach to decisions. Opportunities can be observed early and problems identified more easily, before they become risk factors. Moreover, decisions can be made much easier, based on objective criteria and not on improvisations.

The second advantage is the provision of detailed information and reports that can be used for complex analyses, identifying opportunities for improvement and developing strategies. In order to be able to develop strategies, a lot of information and analysis is needed over several years and from several sources of information. Only in this way will the strategy be viable and in accordance with reality.

The third advantage, increasing the efficiency of the operators, is the saving of time for other activities for the personnel employed, the computer application allowing them to reduce the time to solve the tasks.

The fourth advantage is the access to real-time information, in digital format (softcopy documents), compared to the heavy use of hardcopy documents.

The fifth advantage, in our opinion, is the possibility of standardizing the data entered and their accuracy. It is important, as in any organization, that there should be an equal measure for all, which means standardization. The unit of measurement should not differ from one structure to another.

❖ ***The disadvantages of using a computer application*** are as follows:

The first of the disadvantages is the increased risk of theft and the loss of data, in the softcopy version, due to human errors, or as a result of cyber-attacks.

The second disadvantage, at least for the beginning, until amortized, is an increase in costs, because costs are needed for development, implementation, licenses, maintenance, upgrades, staff training.

The third disadvantage is that the dedicated computer application is conditioned by the construction of an internal network or the Internet connection, which, if it does not work at optimal parameters, can *"mine"* the information.

The fourth disadvantage is the dependence on the further developments of the application, which is important when choosing and contracting the supplier.

The last disadvantage presented, the fifth one, relates to the difficulties in implementing and using the application, due to the complexity or lack of training. As in many cases, human resources make a difference. In order to avoid unnecessary errors, the human resource must be trained and prepared to use the application, which requires time for training.

CONDITIONS REGARDING THE IMPLEMENTATION OF A COMPUTER APPLICATION FOR THE INTERNAL MANAGEMENT CONTROL SYSTEM IN THE MINISTRY OF NATIONAL DEFENCE

Although extremely useful, computer applications are more complicated to implement in the Ministry of National Defence due to specific conditions, especially the need to ensure a data and information security system, a system superior to other institutions. The increased security of data and information automatically entails additional costs in implementation, which could lead to a longer process. However, this impediment to data security can be solved by existing solutions. Of the most viable solutions for the military system, the most appropriate, identified during the research conducted, would be blockchain technology. This type of technology is based on a blockchain that is cryptographically secured and brings a number of benefits that meet the requirements of the national defence system: high security, decentralization, transparency and integrity[3].

Another conditioning could be the lack of personnel specialized in its maintenance, due to the inability of the system to pay the performance differentiated. This service

[3] Nicolae Sfetcu, *Blockchain Technology*, Multimedia Publishing, 2019, Drobeta-Turnu Severin, pp.11-18.

should be outsourced, which entails a possible security risk. Being conditioned by the access to financial resources from the state budget, many implementations in the area of computer applications are still underway. For example, the implementation of the electronic signature. Although there is legislation since 2001, it has not been used yet[4].

The Ministry of National Defence is also part of the state system and, unfortunately, the funds are limited, these being distributed to other objectives considered priority.

Another condition that is felt throughout the budgetary system is excessive bureaucracy. A number of projects are blocked due to excessive bureaucracy: too many signatures; too many documents, sometimes unnecessary; heavy transmission of documents from one structure to another etc.

COMPARATIVE ANALYSIS OF THE MAIN IT SOLUTIONS PRESENT ON THE ROMANIAN MARKET

Currently, on the Romanian market there are several computer solutions designed for the internal management control system in accordance with the legislation in the field, developed by software companies. We have chosen for example three of them, being the most known and used at present:

- Solution e-S.C.I.M.[5] produced by the company SC CONTROL ARHISOFT MANAGEMENT SRL, Str. Gheorghe Grigore Cantacuzino, No. 25 C, Ploiești, Prahova, Code 100010;
- The Gr8SCIM[6] solution produced by the company Ultra Vision SRL, Str. 1 Decembrie 1918 No. 9, Brașov;
- The SMART SCIM[7] solution produced by MOBIUS Software, Str. Doina no. 9, Corp A, etaj 1, sector 5, Bucharest. In the following we will present comparatively the three computer solutions.

Comparative table for three computer solutions by SCIM.

[4] Law 455 of 18.07.2001 on electronic signature, republished in the Official Gazette of Romania no. 316 of 30 April 2014.

[5] See https://e-scim.ro/solutia-e-s-c-i-m/ https://www.youtube.com/watch?v=Z58vBa5A5H8, retrieved on 10.09.2019.

[6] See http://controlinternmanagerial.ro/soft-scim/https://www.youtube.com/watch?time_continue=63&v=e_fI4JHb00Y, retrieved on 10. 09.2019.

[7] See https://mobiussoftware.ro/smartscim/, retrieved on 10. 09.2019.

Criterion/Solution	The solution e-S.C.I.M.	The Gr8SCIM solution	The SMART SCIM solution
Application type: Web, Client server, stand alone.	"It is a web application, authentication being ensured by user credentials and password, accessible in two ways: Connected - Online, by logging in to e-scim.ro; Offline - Offline, by installing the application in the beneficiary entity's data centre, on its server or intranet".	It is just specified that it is a very easy to use computer application, it is accessed with username and password.	The application is based on a collaborative web platform with session security mechanisms and user credentials, web technology, works on any browser with updated security settings. The manufacturing company insists on compliance with security standards and new principles of corporate governance or EU GDPR regulation (for example).
Does it allow the complete administrative approach to the activity of internal managerial control?	NO – It is focused on SCIM documents (which results from the presentation) and does not integrate the management process. The result is a collection of documents similar to any implementation made with this tool. It is focused to ensure the formal compliance of the organization, without managerial utility.	NO – It is focused on SCIM documents (which results from the presentation) – in fact it contains some models of documents, a library of ready-made documents – ensuring self-completion for clients by entering the name of the organization and does not integrate the management process at all. It ensures the minimum formal compliance for the organization that uses it.	YES – Provides a complete administrative framework for the functional implementation and maintenance of an internal management control system – ensures the complete allocation of responsibility, the traceability of the management process of the internal management control, with all its elements, including internal audit mechanisms. It requires the actual work of the managers.
Does it comply with EU Regulation 679/2016 (GDPR) - GDPR ready criterion?	No	No	Yes

Criterion/Solution	The solution e-S.C.I.M.	The Gr8SCIM solution	The SMART SCIM solution
Is the risk management component compliant and applicable in accordance with ISO 31001?	DON'T, load a table in which the risks are recorded.	DON'T, it simulates through a standard document.	YES – The strategic approach to risk management is ensured through the integrated risk management section/component in accordance with ISO 31001.
Does it ensure the integrated management of the procedures of the management control system as well as those of the quality management systems ISO, GDPR, or other standards already implemented in organizations?	NO	NO	YES – The integrated procedure management component ensures the integrated management of all the organization's procedures, regardless of their type, allowing the allocation of a procedure to several categories (e.g. ISO 9001+ ISO 14001+ OHS 18001+ GDPR + SCIM), which can be analysed separately or in context.
Ensures the registration of editions and revisions for procedures, their automatic communication in case of updating and mechanisms for revision, approval, communication?	NO	NO	YES – the collaborative system ensures both the versioning of the procedures, their editions and revisions, the management of the distribution lists, system notifications aimed at updating procedures, their expiration, for example, elaboration/ verification and approval mechanisms, and then automatic communication.
Does the staff evaluate in accordance with the legislation?	NO	NO	Yes, it has a dedicated staff evaluation component, ensuring the correlation between the objectives of the departments of the organization with the individual activities and tasks.

Criterion/Solution	The solution e-S.C.I.M.	The Gr8SCIM solution	The SMART SCIM solution
Does the system comply with the standards associated with the internal management control system?	DOES NOT SPECIFY	DOES NOT SPECIFY	YES – Elements studied and functionally integrated within this solution: COSO Internal Control COSO Enterprise Risk Management Balanced Score Card Enterprise Risk Management ISO 27001/2015 ISO 9001/2015 ISO 31000/2018 EU Regulation 679/2016 (GDPR)
The maturity of the solution – when was it produced/when is it on the market?	over 6 years	6 years	12 years
Is it integrated with other existing applications in the organization?	NO	NO	Yes, the solution is capable of data integration, import and export. Mechanisms for data integration and exchange (web services, XML etc.) are made available to the beneficiaries.
Financial value?	The price is not specified.	It is promoted as having the lowest price.	The price varies depending on the complexity of the implementation in the entity, estimated at each offer.
Support/ maintenance mechanisms/ services	"Offering specialized online support in the adoption, processing, modification, updating and distribution of the documentation of the Internal Management Control System".	"It brings immediate changes to the program according to the legislative changes, this aspect absolving those responsible for additional work".	Online support through the manufacturer's online support centre for implementation, modification, updating, development, complex organization, high added value, updated with the principles of international governance.

Criterion/Solution	The solution e-S.C.I.M.	The Gr8SCIM solution	The SMART SCIM solution
Training services How is it ensured? In what way?	"Training of the personnel of the entity in order to support the process of functioning of the System of Internal Management Control, through the e-learning module integrated in the platform and a specialized online support". The application is actually a registry, the use does not have to be complicated	"The application is designed with a simple, intuitive interface, which can be easily used by anyone, including inexperienced ones. And for any kind of concerns or questions regarding how the software works in the implementation of the operational procedures, the clients can follow the SCIM tutorial on the site". The application is actually a registry, easy to use.	Training of staff at the institution's premises and providing a detailed user manual. E-learning platform dedicated to the application. Training on roles, specific functions for each implementation and the integrations achieved. Readers specialized in training the personnel involved in the internal management control. The application being a collaborative portal, the users have specialized work menus and associated interfaces dedicated to the role within the internal control system, for management there is the section of the dashboard with specific, structured reports.
Training support elements?	Training and training sessions based on two textbooks. Has user manual for the application.	DOES NOT OFFER SOMETHING SIMILAR just tutorial on the site.	User manual and application administration, e-learning system for clients.
Applicability: can be installed/ configured for use in large organizations - involving subordinates, multi-organizational structures?	NO, implementation only for an organization.	NO, implementation only for an organization.	Implementation for an organization or multi-organizational implementation, multilevel, tree, with consolidation of reports, indicators etc.

Criterion/Solution	The solution e-S.C.I.M.	The Gr8SCIM solution	The SMART SCIM solution
How to generate reports?	Automatic generation based on existing documents in the document library.	Automatically autofill institution data in all documents in the document library.	Automatic generation for various types of reporting and teamwork for documents, collaborative system application with levels of reporting correlated with organizational or multi-organizational structure, versioning of documents.
Does it allow the organizational structure to be correlated with the documents?	It proposes adequate ways of managing and implementing the documents specific to the activity field of the entity. Elaborates the organization chart and allocates the specific documents S.C.I.M. uploaded to the platform, on the active compartments in the flow chart.	DOESN'T OFFER SOMETHING SIMILAR.	Has the most complex approach regarding the management of the structure, with a history, direct correlation with ROF, ROI, personal attributions, tasks, responsibilities, personal evaluation.
Duration of implementation	TIME IS NOT SPECIFIED.	It is limited to the elaboration of similar documents, similar for any organization. Under these conditions, the documentation contained for the institution in question replicates in about two hours.	TIMES, depending on the complexity of the entity, estimates between 30 and 120 calendar days are not specified

Criterion/Solution	The solution e-S.C.I.M.	The Gr8SCIM solution	The SMART SCIM solution
Is it dealing with internal audit? Does it provide mechanisms for access and planning, recording and monitoring recommendations for audit missions?	NO	NO	Yes, the solution has a complex component dedicated to internal audit that allows the recording of the entire process – from planning audit missions to reports, recommendations and then monitoring implementation recommendations.

CONCLUSIONS

Following the research carried out, the most complex computer application, existing at the moment on the market, is SMART CIM. Starting from the facilities offered by it, in conjunction with the facilities offered by the other computer applications studied, it was the basis for establishing the requirements for a computer application model dedicated to the internal managerial control within the Ministry of National Defence. Based on the selection made, the requirements of an application dedicated to the internal managerial control for the military organization can be established.

BIBLIOGRAPHY

1. ***, Law 455 of 18.07.2001 on electronic signature, republished in the Official Gazette of Romania no. 316 of 30 April 2014.
2. Nicolae Sfetcu, *Blockchain Technology*, Multimedia Publishing, Drobeta-Turnu Severin, 2019.
3. Dr. Sourabh Sharma & Prof. K.S. Thaker, *Management Information System*, Horizon Books, 2015.
4. https://www.shopify.com/encyclopedia/management-information-systems-mis
5. https://e-scim.ro/solutia-e-s-c-i-m/https://www.youtube.com/watch?v=Z58vBa5A5H8
6. http://controlinternmanagerial.ro/soft-scim/https://www.youtube.com/watch?time_continue=63&v=e_fI4JHb00Y
7. https://mobiussoftware.ro/smartscim

NORWAY – MODEL OF REFORM IN THE MILITARY EDUCATION AND DEFENCE FIELD –

Olivian STĂNICĂ, PhD
Defence Staff, Romania

The Norwegian Armed Forces initiated the educational reform process in 2017, after the Strategy for the period 2017-2020 was approved. Within the military education system reform process, three major goals/challenges were considered: culture, traditions preservation and system reform; administrative and territorial organization, and implementation of integrated educational programs.

The defence reform process began in 2002. In 2018, the Norwegian Armed Forces, together with the Ministry of Justice and Public Security, started the implementation process of a new concept, "Total Defence", based on support and interagency cooperation (civil-military) at national level in crisis, military conflict or war situations.

Keywords: education, reform, security, defence, training.

ADMINISTRATIVE AND GEOGRAPHICAL DATA[1]

Norway is a sovereign and unitary state, governed as a monarchy, with a total area of 385,207 sq. km and a population of 5,382,212 inhabitants. Norway is a founding member of NATO, the UN, the Council of Europe, the Antarctic Treaty and the Nordic Council, a member of the European Economic Area, being also part of the Schengen Area.

Norway is a unitary constitutional monarchy with a parliamentary system of government, in which the King of Norway is the Head of State and the Prime Minister is the Head of Government. The King is Commander of the Norwegian Armed Forces, and head of official diplomacy abroad, as a symbol of unity.

ARMED FORCES STRUCTURE

The Norwegian Armed Forces are subordinate to the Norwegian Ministry of Defence. The Ministry of Defence develops Norway's security and defence policies. The Defence Staff supports the CHOD, and the planning and operational management of military operations are executed by a Norway Joint Command HQ (NJCHQ). The NJCHQ is responsible for planning and leading operations in time of peace, war, crisis, as well as in the Armed Forces international missions.

The Armed Forces include the Defence Staff, the Services, the National Guard, the Rapid Reaction Forces, military education and training institutions, logistical and administrative support structures, with 23,000 military personnel (15,000 in the 3 services + 8,000 conscripts and 10,000 civilians). In the services, the numbers are the following: Land Forces – 8,700 military personnel, Air Force – 2,600 military personnel and Navy – 3,800 military personnel. The National Guard comprises 800 active military personnel + 5,000 military personnel for the Rapid Reaction Forces.

Norway is part of The Nordic Supportive Defence Structures (NORDSUP), a regional cooperation initiative in the field of joint development of military operational capabilities, including: Denmark, Finland, Iceland and Sweden.

THE MILITARY EDUCATION SYSTEM AND REFORM IN THIS AREA

The Norwegian National Defence University College (NNDUC) is the leading military higher education institution that manages and coordinates the initial and continuing training institutions in the Norwegian Armed Forces. The NNDUC

[1] ***, *The World Defence Almanac – 2018,* special issue 2018, vol. XLIII.

is located in Oslo, inside a military fortress (a historical monument, which can be visited by tourists). It has been functioning having the current structure since 2002.

The basic mission of the NDUC is the initial training, specialisation and advancement of the officers, non-commissioned officers and civilian personnel that will be appointed in command structures and military units from Services (Army, Air Forces and Navy), as well as in departments. The NDUC provides individual educational military qualifications for officers and non-commissioned officers (for example: O-4-Lieutenant Colonel – command and staff officer) or individual training certificates for different military branches and specialities (for example: winter training, ground or AA artillery systems, parachute training etc.). The military education and training within the university aims to develop competencies for leadership, military profession, military operations, instructor, military physical training, and specific for each military branch.

As far as the bachelor's degree and master's degree studies are concerned, the specific military fields of scientific research are: military operations and strategies, military leadership, cyber defence, peace support operations, security policies, civil-military relationships, terrorism, conflict resolution, the role of international organizations such as NATO, EU and UN.

The NNDUC[2] coordinates the educational activities for research structures, under the following subordinates: Norwegian Military Academy (Krigsskolen) prepares officers for the Army and those for the Royal Guard; Royal Norwegian Naval Academy (Bergen) prepares officers for the Navy; Royal Norwegian Air Force Academy (Laksevag) prepares officers from the Air Force and the Armed Forces; Command and Staff College, Defence College, Defence Studies and Research Institute with the four subordinate centres (European/Norwegian Security Centre, CIMIC Centre, Asia Area Study Centre, Transatlantic Area Study Centre). At the same time, the military academies also have subordinate schools specific to the Services (Army, Air Force and Navy), as presented in *figure no. 1*.

The commandant (rector) of the university is responsible for the entire educational process of the Norwegian Armed Forces, being also the senior adviser on educational issues to the CHOD.

Within the university, there is also the Technical-Engineering College – TELEMATICS, the University of Physical Education and Sports and the Recruitment and Selection Centre (with 13 locations in the country integrated into the training centres for different military branches/specialities).

The university has 44 specific departments that provide didactic, informational, logistical and organisational support according to the standards of quality assurance of the academic educational process (master studies, e-learning, aeronautical

[2] See http://www.puolustusvoimat.fi/en/national_defence_university, retrieved on 10.06.2019.

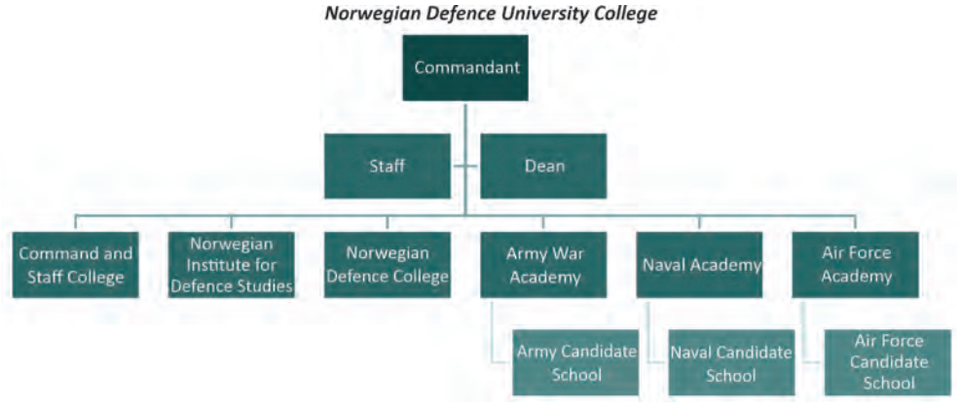


Figure no. 1: Structure of the NDUC

systems research office, library, courses, public relations, education and training, intelligence studies, joint operations, bookstore, legal assistance and humanitarian law, maritime and naval research centre, sociology, curriculum planning, technical assistance etc.).

Within the university, there are programs of bachelor's and master's degree studies (see *figure no. 2*), including career and specialisation courses for officers, non-commissioned officers or civilians from the Norwegian Armed Forces, also with international participation (see *figure no. 3*).

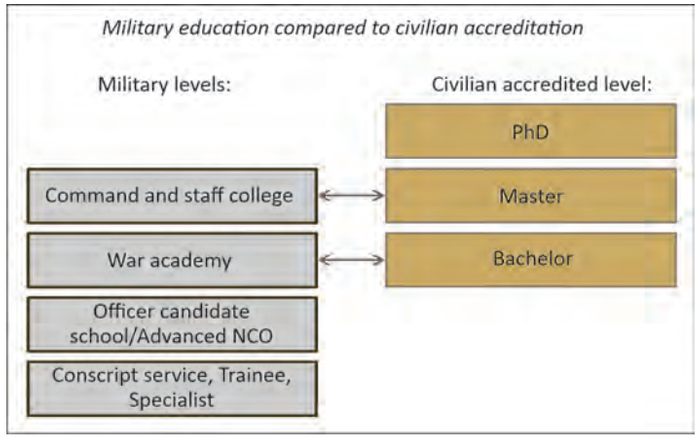


Figure no. 2: University studies programs

Military academies are part of the European Higher Education Area and they have quality assurance systems of the educational process (internal and external) and collaboration/cooperation agreements with higher education institutions, civilian ones, in the country and abroad, within the Erasmus + program.

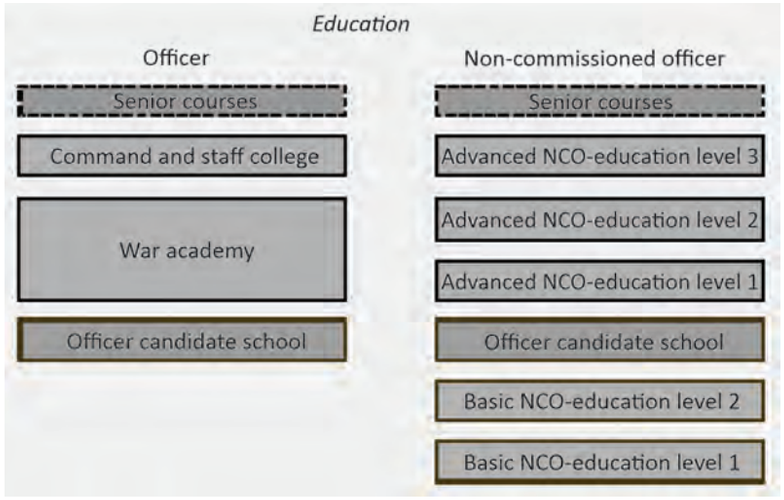


Figure no. 3: Career and specialisation courses for officers and NCOs provided by the NDUC

EDUCATIONAL REFORM WITHIN THE NORWEGIAN ARMED FORCES[3]

The Norwegian Armed Forces started the educational reform process in 2017, after a *Strategy for the period 2017-2020* was approved. Within the process of reform of the military education system, three major goals/challenges were considered: 1. culture and traditions preservation and system reform without affecting the two elements; 2. administrative and territorial organisation, costs cut and quality level improvement; 3. integrated educational programs.

The first objective – culture and traditions preservation and system reform without affecting the two elements:

- within *the Strategy for the period 2017-2020* there were included elements that must be kept in the reform for the continuation of military traditions and aspects of organisational culture (military heraldic symbols and signs, military uniform, military band, commemoration of historical events, battle flags, use and arrangement of former fortresses/fortifications for military events or even for accommodating military institutions – university, academy, school. (See *figure no. 4*).

[3] Colonel Stănică Olivian, PhD, *Report no. SR-1775 on 28.09.2017 following the participation in NATO Training Group – Individual Training and Education Developments,* Oslo/Norway.

Figure no. 4: Culture and military traditions elements

The second objective – administrative and territorial organisation, costs cut and quality level improvement:

- elements of the reorganisation and institutional subordination were included in the *Strategy for the period 2017-2020*. All education and training structures were placed under the subordination of the NDUC: the military academies (with the subordinate military schools), the technical-engineering college – TELEMATICS, the University of Physical Education and Sports, the Recruitment and Selection Centre, and the colleges/schools/centres of training specific to military branches and specialities (infantry, genius, artillery, tanks, communications, CBRN etc.)

Thus, the NDUC Commandant (Rector) ensures the coordination of the entire process of initial training and advancement of the military personnel within the Norwegian Armed Forces in compliance with the quality standards. At the same time, the commandant (rector) of the university is responsible for the entire educational process of the Norwegian Armed Forces, being also a senior adviser on training and education issues to the CHOD (see *figure no. 5* and *figure no. 6*).

The third objective, integrated educational programs:

- *The Strategy for the period 2017-2020* included elements of reorganisation of the educational curriculum, respectively integrated programs, of *"joint"* type, at the bachelor's and master's degree studies level, integrated programs for the continuous training of officers and non-commissioned officers for different functions of command or different military branches and specialities. For now, it seems that the hourly planning is deficient (the teaching norms, the distribution of teachers, instructors in different teaching activities, seminars, laboratory, ranges etc.) to support certain programs of specialisation and advancement for the officers and non-commissioned officers due to the large distances between Oslo (where the university is located) and the other education/training facilities in Krigsskolen, Bergen, Laksevag (academies, colleges, schools, training centres etc.).

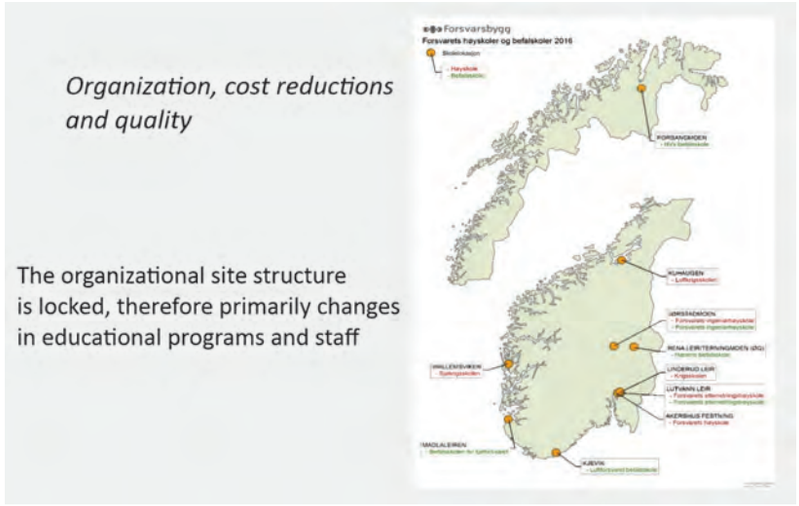


Figure no. 5: The administrative and territorial organisation and location of the education and training structures from the NDUC

Figure no. 6: Integrated educational programs

The advantages of implementing these strategies in the educational field are: cutting the costs in the financial area, integrating the study programs and enabling the *"joint"* level for the graduates of university and master studies, eliminating bureaucratic aspects when getting certain documents approved by different decision-makers and simplifying the decision-making process under the authority of the Commandant of the NDUC, who is also the main adviser on training and education issues to the CHOD.

DEFENCE REFORM – *"TOTAL DEFENCE"*[4] CONCEPT

The process of reform in the field of defence began in 2002, following the recommendations of the Norwegian Parliament no. 234 (2003-2004) for the Defence White Paper no. 42 (2003-2004), in which the broadening and modernisation of the *"TOTAL DEFENCE"* concept was approved, including: mutual support and cooperation between the Norwegian Armed Forces and the civil society in connection with contingency plans, crisis management and the consequences of crisis management – from peace through political security crises to armed conflict.

In 2018, the Norwegian Armed Forces, together with the Ministry of Justice and Public Security, started the implementation process of the concept of *"TOTAL DEFENCE"* (Support and Cooperation – a description of the total defence in Norway), based on support and interagency cooperation (civil-military) at national level for crisis, armed conflict or war situations.

Within this concept of *"TOTAL DEFENCE"*, there were laid the foundations of cooperation (including from a legal point of view) between the governmental or non-governmental organisations, at national or international level, which have the capacity to deploy forces and resources in the field and must provide support to the civilian population in emergencies, terrorist attacks, lethal or non-lethal weapon attacks, hybrid threats, war or armed conflict.

The tools included in this concept of *"TOTAL DEFENCE"* are: governmental agreements between public institutions and agencies, coordination and functioning mechanisms for crisis management (from peacetime through political crisis to armed conflict) built according to laws, regulations, royal decrees, military or civilian orders.

The main actors in this concept are: the relevant ministries within the government, the civil society (the municipality, the civil protection, the regional governor, the police, the civil society organisations in the field of logistics, infrastructure, energy etc.) and other international organizations such as NATO, UN, EU, OSCE, RED CROSS INTERNATIONAL.

The concept of *"TOTAL DEFENCE"* is based on the resources of civil society, trade agreements, cooperation with civil authorities that will be used in the event of armed aggression for the defence of the nation. At the same time, Norway's defence is built on both military defence and civil society preparation for crisis or war situations. Crisis management and coordination of agencies at central

[4] See http://www.publikasjoner.dep.no, retrieved on 22.07.2019.

level is performed by a number of institutions, such as: Parliament, Government, Government Security Committee, Office of the Prime Minister, relevant ministries, Emergency Council, Support Unit for Emergency Situations.

The military forces, according to NATO documents, are dependent on the civilian sector such as: transport (90% of military transport use open trade routes), information (50% of military stations used for military purposes are from the civilian commercial sector) or HNS operations (over 75% of the products – food/water – requested by the military forces are supplied by civilian agencies or use civilian infrastructure). Essentially, the Norwegian Armed Forces have become much more integrated into the civil society as a source of skills, supply of goods and services, including for advanced technologies.

At the international level, in conceptual terms, for Norway, *"TOTAL DEFENCE"* includes traditional regional cooperation with countries belonging to the Nordic community, such as: Denmark, Finland, Iceland, Sweden, and this cooperation involves efforts to promote democracy, respect international laws and human rights, gender equality and development support. The ministries of the respective countries are constantly discussing the potential of risks such as: natural or man-made disasters, terrorist or cyberattacks, as well as the ways in which they can provide mutual support in accordance with their own defence and security cooperation plans, complementary to the cooperation in NATO's formal framework.

Norwegian MoD[5] tested this concept in 2018 in the *TRIDENT JUNCTURE-18* exercise for which it used commercial vessels from civilian companies. For example: civilian shipping company Simon Mokster provided, during the exercise, a seagoing ship that had a mixed military-civilian crew. The ship was used as a platform for maintenance, fuel supply and logistical support for the military actions of the Norwegian Naval Forces at sea. This concept of civil-military cooperation in the maritime field is called *STOFT (Ship Taken Out of Trade)*, which involves taking/removing a civilian ship from normal operations and using it in support of military departments at sea. At the same time, during the year, the Norwegian Armed Forces and the Norwegian Department of Civil Protection tested certain standard operating procedures for emergency, search and rescue at sea and land in case of disasters or natural calamities.

The Norwegian model was also adopted by Sweden[6], which developed the concept of "*TOTAL DEFENCE"* in two directions: military defence and civil defence.

[5] See http://sidinfo.com/2018/12/norway-trident-juncture-2018-and-the-total-defnce-concept/, retrieved on 29.07.2019.
[6] See http://www.government.se/articles/2018/05/development-of-modern-total-defence/, retrieved on 30.07.2019.

Within the National Defence Strategy approved in 2015, there were three major challenges for civil defence, as follows: *a. the coordination of the so-called grey zone and of the transition from the organisation of society in peacetime to the state of war; b. the integration of the civil defence into the current emergency preparedness system; c. the approach to different objectives of civil defence in order to strengthen cooperation with the Armed Forces*. These challenges remain valid and are relevant to the concept of *"TOTAL DEFENCE"* developed by the Swedish Armed Forces.

Currently, Sweden aims to revitalize the concept of total defence, and the first stage will be the development of the potential for resistance in the non-military component, according to the latest government report, entitled: *Resilience – the Total Defence Concept and the Development of Civil Defence 2021-2025*[7]. This document (strategy) includes new threats related to cyber space and the digitisation of social life. The strategy also strengthens the citizen's independence from the support of state institutions or civil agencies in the event of a major crisis. The implementation of the concept of total defence will be based on the cooperation between the Swedish Armed Forces and the Swedish Agency for Civil Contingencies, including by reviewing the *Law on protective security*, implementing the national intelligence and cyber security strategy, ensuring a consolidated budget for investment in military and civil agencies, signing political agreements for cooperation and cooperation between different civil agencies and departmental structures in crisis or armed conflict situations.

CONCLUSIONS

The military education reform initiated by Norway will probably ensure, over a 10-year horizon, cost efficiency, maintaining quality assurance standards in education, and it will simplify and optimise the act of command. The model could be used by other nations for future strategies or doctrines in the field.

The educational component is part of the training process of the human resource for the Norwegian Armed Forces, and the integration of the university/post-university study programs within the National Defence University (NDUC) will probably optimise the process of organising and conducting the joint type programs for the command and staff officers in the three military services.

The concept of *"TOTAL DEFENCE"* can be assimilated to the concept of *resistance war* or *popular war in the modern version*, with the application of some principles

[7] See http://warsawinstitute.org/swedish-total-defence/, retrieved on 29.07.2019.

(it becomes more and more used in NATO) in order to be ready for military actions of the type of *short of war* or *the long war*. For such versions, it seems that military actions will be carried out only by the military forces and the specific means available, prepared in the peacetime, without supplementing or mobilising other forces and means. In my opinion, countries that opt for this kind of war should overcome the deadlock from the initial period of the war/military conflict and subsequently develop military/civilian capabilities for the long war (this is the role of the military/civilian interagency cooperation in support of the long war).

The Norwegian Air Force, after the implementation of *"TOTAL DEFENCE"*, will have the necessary support for developing the new defence planning documents (defence white paper, military strategy) in the short and medium term, depending on the threats and vulnerabilities to the future security environment.

In my opinion, the interagency cooperation at national level (in Norway) would not have been possible without the two ministers (of defence, and justice and public security) signing and promoting the implementation plan of the total defence concept in 2018. At the same time, the financial resources allocated to the development of new military and civilian capabilities can be targeted and streamlined in order to achieve a common purpose, namely: to defend the territorial independence, the sovereignty of the country, and the civilian population without duplicating economic efforts or wasting (sometimes without justification) investments in different top areas, such as: information systems, critical infrastructure, cyber defence etc.

The concept adopted by Norway could be a model for NATO/EU member countries in the organisation of their own security and defence systems, where all state institutions with responsibilities in the field of national security unite their capabilities and can respond to a situation of crisis or they can carry out a military conflict/war in the short or medium term without international support.

BIBLIOGRAPHY

1. ***, *Strategy Journal: Norway, Trident Juncture 2018 and "Total Defence Concept"*, October 2018.
2. ***, *Support and Cooperation – A Description of the Total Defence in Norway,* the Norwegian Ministry of Defence and Norwegian Ministry of Justice and Public Security, 2018.
3. ***, *The World Defence Almanac – 2018,* special issue 2018, vol. XLIII.
4. Colonel Olivian Stănică, PhD, Scientific Paper: *"Studiu comparativ al sistemului de învăţământ militar din armata României cu cel din statele membre NATO"*, defended on 28.11.2013 within the Doctoral School, *"Carol I"* National Defence University.

5. Colonel Olivian Stănică, PhD, *Report no . SR -1775/ 28.09.2017* following the participation in *NATO Training Group – Individual Training and Education Developments, Oslo/Norway.*

WEBOGRAPHY

1. http://www.publikasjoner.dep.no
2. http://www.puolustusvoimat.fi/en/national_defence_university
3. http://sidinfo.com/2018/12/norway-trident-juncture-2018-and-the-total-defnce-concept/
4. http://www.government.se/articles/2018/05/development-of-modern-total-defence/
5. http://warsawinstitute.org/swedish-total-defence/.

QUO VADIS ROMANIAN DEFENCE INDUSTRY

Lucian IVAN, PhD

"Alexandru Ioan Cuza" Police Academy, Bucharest

On 19 March 2019, the European Union's governing bodies approved consistent programmes for the period 2019-2020, totalling more than 500 million EUR, which are designed to ensure co-financing of projects developed by the defence industry within the EU Member States.

At the same time, from 2021 onwards, the European Defence Fund is to be launched, an innovative and competitive programme for the defence industry, which will substantially contribute to the strategic and military autonomy of the European Union. These unprecedented financial efforts for the defence industry of EU member States are part of the conjugated efforts to defend European citizens from possible hostile actions of certain state and non-state entities.

Considering these consistent investment opportunities, Romania must be prepared to cooperate with major European companies in the defence industry, in order to develop viable projects that are eligible to be funded through the European Defence Fund. Also, a priority of the Romanian defence industry must be a substantial increase in research investments, an immediate result of increasing the competitiveness of the products achieved and, implicitly, increasing the volume of military equipment exports to the profile markets.

In view of these objectives, Romanian companies operating in the defence sector need to invest considerable sums in the field of research, in order to develop high-performance military products and technologies that enable the development of this field of strategic interest for Romania. Another opportunity for the Romanian defence industry is to provide the necessary facility to produce military equipment and technology meeting NATO standards, in order to be used by the Romanian army.

In this context, the Romanian defence industry is expected to face great challenges in the future, the major opportunity and strategic advantage being the special relationship with NATO and EU partners, in particular the strategic partnership with the USA.

According to the commitments assumed, at political and military level, the Romanian Government will invest in the next years, in the defence sector, 2% of GDP, a large part of this percentage (over 20%) to be allocated to products that encompass advanced technologies, most of which are to be imported from EU and NATO member states, as well as from the local market.

Keywords: defence industry, technology, European Defence Fund, investment, research.

This work was carried out with the support of the POCU 125040 project: *"Development of tertiary university education in support of economic growth – PROGRESSIO"*, Project co-financed by the European Social Fund, Human Capital Operational Programme 2014 – 2020.

INTRODUCTION

At the global level, the transition from the *"classic"* war to the hybrid war that entails major security challenges, given its specificity. Hybrid warfare is characterized by the component of aggression at informational level and the high degree of unpredictability of actions carried out by the opponent, which induces complex threats characterized by asymmetry.

The complex and non-linear threats specific to hybrid warfare have direct effects at the level of the operational requirements of the defence industry, and it is necessary to achieve rapid and continuous adaptation of this strategic economic sector to the risks and threats induced by non-conventional aggression. In this context, an important emphasis is placed on the illegal and aggressive actions of the Russian Federation, which have affected the geopolitical and geostrategic structure in Romania's vicinity.

In this particularly unpredictable geostrategic context, NATO, the EU and Romania must consider the continuous growth of the military forces belonging to the Russian Federation in the Wider Black Sea region, especially after the illegal annexation of the Crimean Peninsula and the aggressive actions of a hybrid nature in Ukraine.

At the same time, the Kremlin's ambitions in the military field are reflected in the Gerasimov Doctrine 2.0, which was launched at the beginning of 2019 by the Chief of Staff of the Russian Federation Armed Forces, consisting in changing the priorities of the Russian Defence Industry, in the sense of developing modern weapons systems to cope with any challenges of a security nature. The declared objectives of the Russian Federation consist in annihilating NATO's defensive capacities, including the Romanian elements of the Missile Shield (Deveselu), which must be carefully analysed by military experts, to react in a timely manner and to effectively counteract these aggressive intentions.

From the data publicly expressed by Russian officials, by the year 2025, the Russian Federation intends to produce 30 modern battleships for the equipment of the Black Sea military fleet, with a consistent financial effort (over 2 billion USD). This confirms the strategic priorities of Moscow, which intends to invest large amounts of money in modernising military capabilities in order to be able to perform operations in the Black Sea area, one of the objectives specifically targeted, being Romania.

At the same time, after the illegal annexation of the Crimean Peninsula, the air force has been deployed in this area, increasingly testing the responsiveness of NATO forces, by frequently violating the airspace of NATO states in this region, in particular that of Romania. Modern missile systems have also been deployed in the Crimean Peninsula, which can hit targets in NATO member states, notably Romania, Bulgaria and Turkey.

In the context of the military intervention of the Russian Federation in Syria, the Black Sea military fleet has great strategic importance for operations in the eastern Mediterranean, respectively for the support of Russian expeditionary forces, given the fact that the military infrastructure in the Crimean Peninsula has been important for the logistical support of the Tartous base in Syria.

In the context of these new asymmetric challenges, the Romanian Armed Forces have undergone an important process of planning its procurement, based on the premise that *"defence begins at home"*. This modern and effective approach has been appreciated by NATO partners, given that in the event of an armed aggression, the first forces used in the conflict will be the national ones, until the arrival of the Alliance troops for the defence of partners, as stipulated in Article 5 of the NATO Treaty.

At NATO level, in the current global and regional security context, Romania's role is strategically important and appreciated as an observation outpost (detection sensors, information gathering), logistic outpost (interoperability with NATO's pre-positioned troops and equipment) and early defence (rapid reaction systems capable of annihilating hybrid, asymmetric, cyber-attacks).

CHARACTERISTICS OF THE ROMANIAN ARMS MARKET

Before the Revolution of 1989, the Romanian defence industry held about 100 enterprises in which approximately 130,000 employees worked, and arms exports exceeded 800 million USD, with our country in the top 10 states exporting military equipment.

Following the successive reorganisations occurring over the past 30 years, 22 companies with full state capital are currently operating, 15 of which belonging to CN ROMARM SA, a national company subordinated to the Ministry of Economy, and the private security industry is represented by 17 companies. The disappearance of more than 50% of the arms-producing facilities is due to the loss of traditional markets for the military equipment provided by them, as well as their malfunctioning, including the background of lack of flexibility and adaptation to international arms market requirements. Another feature of the Romanian defence industry is the continuation of the production of Eastern type weaponry and the transition

towards NATO-compatible systems was made after a long period of time following our country's joining the North Atlantic Alliance in 2004.

From the analysis of publicly available economic data, it follows that the part belonging exclusively to the Romanian state needs an objective assessment of the potential for development and a structural restructuring that is based solely on a coherent and objective economic analysis, without political or trade unions interference. Currently, there are companies that are at the limit of bankruptcy, especially because of lack of orders, but there are certain companies that have consistent export contracts. However, they cannot meet the customer requirements, given the lack of qualified personnel and outdated technologies that do not allow for the proper growth of production.

At the same time, some companies carrying out similar or identical activities need to merge, but there is the temptation of the management of these companies to maintain boards of directors where an important percentage of members are designated exclusively on subjective criteria, as a reward for services of an arbitrary nature, not having the necessary professional and technical qualifications to make decisions in order to support those undertakings. In addition to these issues, a very important factor in the decision-making process to maintain the facts is represented by trade unions in the defence industry, which oppose the reorganisation based on the efficiency of certain companies that no longer have possibilities of economic recovery. Trade unions in the defence industry must be an important factor in the recovery of the defence industry, with the role of proactively signalling certain dysfunctions at the level of the component entities, and the deciding factors are obliged to analyse carefully their requests and take appropriate measures to be economically substantiated. Professional retraining programmes, including entrepreneurship, should also be initiated at governmental level, concurrently with measures of a fiscal nature that encourage the development of new business, to reduce the pressure of the social nature.

Another factor contributing to the economic incapacity of the domestic defence industry consists in the lack of modern production technologies, military equipment and armaments currently being manufactured with technologies developed predominantly in the period 1960-1980, being assimilated in particular to the know-how of Soviet origin, which is reflected negatively on the quality and competitiveness of military products, especially in the external market. Currently, the external arms market develops at an accelerated rate, with large companies in the field investing important amounts of money in the development of modern technologies tailored to the requirements of beneficiaries, with potential in emerging markets, especially in the Middle East and Asia.

Another aspect that leads to the inefficiency of an important part of the indigenous defence industry consists in the chronic underfunding of the defence industry for several years, as well as the lack of predictability of the expenditure allocated to the equipment and training of the Romanian Armed Forces. Another very important area consists in ensuring the maintenance of the military products that has been affected by the redistribution of financial resources to other areas, having also consequences on the private component of the defence industry, which has lost orders to execute maintenance for certain military products, with repercussions in the financial stability of these companies. The maintenance of the products imported and used by the Romanian Armed Forces is required to be mentioned in off-set contracts, and these operations are carried out in our country by domestic companies that collaborate with exporting entities, including by fetching their know-how. The realization of this partnership will make the technological transfer to Romanian companies, including in terms of modern management of defence business.

An important component that has contributed to maintaining an acceptable level of the Romanian defence industry is constituted by the arms exports that have evolved as follows: 2010 – 163 million USD, 2011 – 180.8 million USD, 2012 – 106.1 million USD, 2013 – 235.1 million USD, 2014 – 211.3 million USD, 2015 – 176.6 million USD, 2016 – 186.1 million USD.

Although the figures related to arms exports are at an acceptable level, in many instances there were cases of orders that were not honoured on time, amid the use of outdated technologies, as well as the acute lack of specialised staff. The lack of specialised personnel is due to its ageing and early retirement, but also of highly skilled labour migration to the non-military private sector. To solve this problem, it is necessary to revise the staff policy at the level of the companies within the Romanian defence industry, including by modifying the way in which the motivation of employees is undertaken and the promotion solely based on the criteria of professionalism. In this context, the subjective criteria for the promotion of staff should be eliminated, and at the level of the company's management the selection should be made exclusively on objective criteria, based on a mandate contract not exceeding four years. In order for these objectives to be attained, measurable and quantifiable tasks should be explicitly stipulated in order to be monitored periodically by the members of the Management Board and the corrective action can be taken in real time in order to streamline business activities.

From the point of view of physically and morally outdated technologies, this is mainly due to the lack of a coherent strategy, backed up by state policies, to redevelop the defence industry sector, including the investment component based on economic efficiency. In the medium and long term, a limitation of Romanian

arms exports and, implicitly, the insolvency or even bankruptcy of certain companies in the profile market can be anticipated, under the conditions of such failures persistence. To avoid this scenario, it is necessary for the governmental decision-makers to understand the role that the defence industry plays in the technological development of society as a whole. It can also be adapted for the civil industry, and the results of scientific research in the military field can contribute to the technological development of Romania. In this context, the relations between the defence industry and academia and research should be defined, and certain projects that are considered strategic can be developed in public-private partnerships, including by attracting funds non-refundable from external sources through the European Defence Fund.

This can be linked to the fact that, in recent times, Romania has allocated low financial resources to the research and development sector in the arms industry, the achievements in this area being largely due to the human factor that, being passionate about the work carried out (intrinsic motivation), accepts to create and innovate in a non-performing system.

In this context, on 29 February 2019, the representative trade unions of the arms industry asked the Presidential Administration to support the development of a defence industry research centre, focusing on research and development capacities, capable of providing access to European funds[1]. These important proposals for national security and their economic and social impact have been forwarded to the Romanian Government, the Ministry of Economy and the Ministry of National Defence[2], in order to analyse their appropriateness in the current economic and social context. These proposals are appreciated as viable by trade unions but present the specific disadvantages of centralising research and development activity, with effects in the management plan of this entity. From an organisational point of view, the optimal variant may consist in the development and consolidation of cooperation relations between the existing research institutes and the academia, as well as the joint application to projects financed by EU funds, including by accessing the amounts of money that will be made available through the creation by the European Union of new modern financing instruments (e.g. the European Defence Fund).

In order to access these financial instruments, it is necessary that the defence industry entities and the military research institutes should adapt their own policies to achieve partnerships with strong companies in the community area, with the aim

[1] See https://www.fonduri-structurale.ro/stiri/21714/se-urmareste-realizarea-unui-centru-de-cercetari-al-industriei-de-aparare-inclusiv-prin-accesare-de-fonduri-europene, retrieved on 25.10.2019.

[2] See https://www.libertatea.ro/stiri/sindicalistii-din-industria-de-aparare-au-mers-la-cotroceni-2559266, retrieved on 25.10.2019.

of maximising the chances of accessing consistent financial resources contributing to the modernisation of the national defence industry.

The statistical data available in the online environment reveals that, *"in the year 2015, the MoD budget earmarked for research & development domain was 2.67 million RON (approximately 670,000 USD), in 2016, 1.15 million RON, and in 2017, approximately 1.2 million RON, while states close to Romania, such as Serbia, annually invest about 3 million USD"*[3]. The level of investment in military research reflects the interest of government factors regarding the defence of the national territory against possible external aggression, as well as the degree of technological development of society, considering that military technologies induce positive effects including at the level of Romania's development.

If, by the year 2017, the lack of material resources was invoked, by allocating 2% of GDP to military expenditure, which was assumed at political level by concluding an agreement between all ideological formations with parliamentary representation, this reason cannot be invoked at this time. The main problem now lies in the way in which these funds are allocated on budget chapters, depending on the priorities identified at national level. At present, at the level of the Ministry of National Defence, there is a relatively low interest in military research, which will lead to the delay of consistent research projects with final impact on the modern equipment of the Romanian Armed Forces, as well as on the profile industry and arms exports. The purchase of modern military equipment from external markets can be a viable solution only in the short term, given their very high costs, as well as the long-term cost for maintenance, amid the lack of local expertise in this respect. An important opportunity for the Romanian defence industry can be the transfer of know-how from exporting companies to the indigenous ones, in order to achieve maintenance by Romanian entities, by extending strategic partnerships with large companies in the Euro-Atlantic area.

Another aspect of interest is the weak and non-compliant cooperation between the Ministry of National Defence and the Ministry of Economy, amid the non-approach of common research and funding themes, jointly, of relevant programmes on the national security. This communication dysfunction is reflected directly at the level of the defence industry, given that many companies belong to the Ministry of Economy, through the CN ROMARM SA, and the beneficiaries of these products are the military units of MoD. In order to overcome this institutional syncope, it is necessary to achieve a real partnership between the two ministries, including by making a direct communication on all management sites. This can be surmounted

[3] See https://newstrategycenter.ro/wp-content/uploads/2016/04/2017-Martie-Ap%C4%83rare-%C8%99i-Industrie-studiu-New-Strategy-Center.pdf, retrieved on 25.10.2019.

by communicating the strategic aspects between the two ministries, including by engaging the Prime Minister of the Romanian Government and its working apparatus in this extremely important area.

An important role for accelerating cooperation in the field of defence industry has the Country's Supreme Defence Council, a body where all relevant actors can contribute to the development of the defence industry. Coherent medium- and long-term policies that can prove their usefulness in the recovery of the national defence industry can be adopted under the coordination of the Presidential Administration and the Romanian Government.

Specialists in the field also appreciate the need to intensify cooperation between the state and private sectors in the field of research and development of military products and technologies, including through the active involvement of the Government and Parliament role in creating the legislative framework and the public policies necessary to support this endeavour. Currently, in the private defence industry, important sums are invested in projects under the field of applied research in the military sector, the funds allocated being much higher than the funding from the state budget. A relevant example is the private investment for the development of unmanned military flight systems or in the area of specialized software development for military communications systems. In fact, Romania has a remarkable potential in the IT&C area, which can be exploited by the defence sector, including by assigning military research themes, which can also be capitalised on in the external arms market, thereby obtaining important sums that can be reinvested in the defence industry.

However, in the year 2019, according to the declarations of the Minister of Economy, *"the defence industry has 10 times the execution budget of the previous year, and a much larger project is being linked to value chains"*[4]. This is very important because, by making connections between value chains, financial bottlenecks are avoided, with positive effects at the level of financing relevant projects and timely implementing current payments (e.g. payment of utilities, payment of wages).

Another important aspect is merging productive units with the same activity profile, in order to avoid redundancies in the profile market as well as to streamline the management activities. An example in this respect is merging the powder plant in Făgăraş and Pirochim Victoria, the Romanian Government allocating, according to the declarations of the Minister of Economy, the sum of 173 million RON.

Another desiderates assumed at the level of the Ministry of Economy consists in the implementation of modernisation projects at UM Cugir and UM Sadu. It should

[4] See https://www.investingromania.com/ro/stiri/stiri-agerpres/b-d-l-u-industria-de-ap-rare-are-de-10-ori-bugetul-de-execu-ie-de-anul-trecut, retrieved on 25.10.2019.

be noted that, at present, UM Cugir has secured arms exports to the USA for about 25 million EUR, and for the performance of these important contracts, consistent investments are needed in increasing the production level, both at quantitative but mostly qualitative levels.

There are also concerns to develop relations with the Italian arms company Beretta to produce the ARX 160 weapon and a smaller NATO calibre weapon for special troops. In this context, the Romanian official noted that *"less than 10% of what produces the domestic defence industry is purchased by the Romanian Armed Forces, while at the level of the European Union member states, the mean percentage is about 70%, in France the percentage being 100%"*[3]. This must be analysed from the perspective of the Romanian Armed Forces procurement policy, which is obliged to comply with NATO standards, and the large procurement projects under national law must be won through a transparent process of public auction. In order to be able to access the funds allocated to the defence industry, it is necessary to analyse its potential to produce the necessary products for the armed forces, also through the possibility of participating in these auctions in economic partnerships, including relevant actors in the arms market in the North Atlantic area. It must be considered that the Romanian Armed Forces have an obligation in NATO to equip themselves with modern assets comprising state-of-the-art defence equipment and systems that the domestic defence industry is currently unable to provide. In this context, the only solution for accessing a major part of the funds allocated from the state budget for the purchase of military equipment and systems is to maximise the use of off-set contracts whereby companies delivering Romanian military products should be obliged to invest some of the amounts obtained from the award of contracts in the domestic industry in the field.

At the same time, the development strategy of the national defence industry must take into account the fact that the market to which it is addressed is the result of requirements due to potential risks and threats, as well as the missions assumed by the Romanian state at NATO level (expeditionary component, information, early warning). In this context, it is necessary that the managers of the national defence industry companies continuously adapt their economic development policies, considering trends in the arms market at national and international level. In this regard, it is useful to invest funds in the conduct of complex market analyses that provide managers with the best economic and investment solutions, meeting the internal market requirements, as well as those of emerging markets in continuous development.

At the moment, the Romanian Armed Forces have ensured consistent funds from the state budget, including for procurement, given that at national level it was agreed to guarantee a national political consensus between all the parliamentary parties

that oblige, irrespective of whether they are in power or in opposition, to respect the firm commitment to support budgetary allocations for the Romanian Armed Forces at a steady level of at least 2% of GDP for the next 10 years. At the same time, the support for the multiannual budgetary planning of military expenditure was agreed to ensure the predictability of Romania's military procurement policy with modern combat technology, as well as the development of cooperation projects between the national defence industry and profile companies in other states.

At the same time, the Romanian Armed Forces allocated about 23% for the procurement of combat techniques from the budget allocated to the MoD, with the prospect of achieving 40% in the future, which falls within the NATO recommendation that the procurement part is not less than 20% of the total funds allocated to military expenditure.

In this context, the entities within the indigenous defence industry can forecast their budgets according to the operational requirements of the Romanian Armed Forces, including considering the export potential in the profile markets. In fact, the *"engine"* of the Romanian profile industry development may be represented by the exports of armament and military equipment, but account should be taken of the developments on these markets, namely the demand for military equipment of the states with consistent financial resources that massively invest in military technology change.

Thus, analysing exports on the profile markets of the year 2018, based on publicly supplied data by the ANCEX Control Department of the Ministry of Foreign Affairs (www.ancex.ro), the first 10 Romanian arms clients were: *"United States of America – 72.31 million EUR; Bulgaria – 27.76 million EUR; Tunisia – 23.77 million EUR; Israel – 22.43 million EUR; Saudi Arabia – 7.83 million EUR; Switzerland – 6.24 million EUR; Afghanistan – 4.67 million EUR; Czech Republic – 4.12 million EUR; UK – 3.94 million EUR; Guinea – 3.66 million EUR"*[5].

By analysing this data, we can say that Romanian exports of military products cover the most relevant international markets, but considering the products exported by Romanian companies, they contain obsolete technologies (being produced with technologies from the years 60-80), still relying on Soviet licenses. On Soviet-type weapons licences, the Russian Federation has repeatedly warned Romania, in international fora, on the fact that the licences purchased during the Cold War have expired and a new terms of production licences must be negotiated.

At the same time, from the analysis of this ranking we can note that Romania has lost important traditional markets in Africa and the Middle East. In this context, it is necessary to carry out a fair and complex analysis of the objective and subjective

[5] See www.ancex.ro, retrieved on 25.10.2019.

causes that have led to the loss of these international markets and to restore the necessary contacts to regain them, including through the active involvement of the relevant ministries, namely the Ministry of Economy, the Ministry of National Defence and the Ministry of Foreign Affairs.

In the light of the abovementioned issues, we can state that these exports to those destinations are not economically viable in the long term, in the absence of viable programmes and relevant analyses contributing to the modernisation of equipment and armaments produced by the companies within the national defence industry. Taking into account the increased demand for modern weaponry in the external profile market, the increase in Romanian arms exports can be achieved through cooperation with profile companies, including through the realization of joint ventures or privatization by attracting economic organisations with high financial and technological power from EU and NATO member states.

SYSTEMIC DYSFUNCTIONS AT THE LEVEL OF THE DEFENCE INDUSTRY

Based on the analysis carried out at the level of the indigenous defence industry, certain systemic dysfunctions have been identified which are directly reflected in the profitability of this area of national strategic interest, namely:

a. The major difference in the technological level between Romanian companies from the defence industry and external competitors

In order to cope with this technological gap, it is necessary to identify certain opportunities for Romanian products in the international profile market, leading to increased arms exports, while achieving partnerships with certain profile companies to support the process of achieving, in partnership, products that encompass cutting-edge technologies. This latter issue will allow the transfer of know-how to the Romanian profile companies, which will benefit from this technological advantage for the consolidation of business undertaken in partnership with the major companies in the international arms market. At the same time, the transfer of know-how will allow the specialisation of the staff working in the defence industry with the latest technologies on the market, while streamlining how production activities are underway (e.g. new streams technology).

b. Human resources that no longer correspond to the current technological requirements

The human resources issue can be surmounted by providing financial incentives to the staff operating in the defence industry, including through fiscal measures, like those granted to the staff working in the IT industry. These tax-related facilities can be justified in the face of European fora, through the strategic nature

of the defence industry, the argument being an increase in the European Union's means of defence by dynamizing this sector of activity at the national level. In the long term, it is necessary to reduce the personnel carrying out hazardous technological operations (e.g. explosives factories) by automating these technological processes, while allocating the human resource made available to other activities within the company.

c. Exporting products that encompass obsolete technologies

Based on the analysis of the data made available on the website of the ANCEX Control Department (www.ancex.ro), Romanian arms exports are, during the last period, on an upward trend. However, based on the analysis of the export structure weapons categories, Romania exports morally outdated military equipment. This will lead, in the medium and long term, to limitations in business figures obtained by exporting companies, given the sharp dynamics of the international arms market.

d. Lack of a coherent financing mechanism for multi-annual procurement programmes

Currently, although measures have been ordered at the level of the Ministry of National Defence for the design of multi-annual procurement programmes, the amounts of money allocated for each programme are not accurately known, which affects both the state industry and the joint or private capital. In order to carry out profitable economic activities, there is a need for contextual transparency, in the sense of the correct information of the economic entities within the national defence sector on investment opportunities that can be generated by the implementation of the Romanian Armed Forces major procurement programmes.

e. Poor drafting of specifications for the Romanian Armed Forces major procurement projects

According to the data provided by The New Strategy Centre, *"the practice of too ambitious or realism-free operational requirements in relation to existing resources has finally made the army equipped with excessively expensive products, the interoperability of the products being questionable"*[6]. In order to resolve this deficiency, it is necessary to specify strictly the operational requirements for the conduct of the missions undertaken by the Romanian Armed Forces at national level and in the context of NATO. Regarding interoperability, it is necessary to carry out coherent analyses enabling the operational requirements to be compatible with the military equipment held by the other NATO member states in order to have coordinated actions in the event of an armed conflict caused by a third state.

[6] See https://newstrategycenter.ro/wp-content/uploads/2016/04/2017-Martie-Ap%C4%83rare-%C8%99i-Industrie-studiu-New-Strategy-Center.pdf, retrieved on 25.10.2019.

f. The chronic underfunding of military research from budgetary funds and the difficulties in public sector-private sector cooperation, with no coherent inter-agency strategy to determine the development of research and development in the analysed field.

COOPERATION AT INTERNATIONAL LEVEL IN THE FIELD OF DEFENCE

In order to modernise and streamline the national defence industry and ensure its sustainability in the medium and long term, cooperation measures are needed with major defence industry companies, especially those in the Euro-Atlantic area. The cooperation with major global profile companies brings tangible benefits to the indigenous defence industry by transferring know-how, training staff to high technological standards, and conducting business on national territory, by transferring production facilities to our country.

In this context, in order to facilitate international cooperation, it is necessary to consider the following minimal set of measures leading to the achievement of this strategic objective, namely:

- Romania's active participation in the multinational projects, including by accessing European funds available through the EU funding mechanisms, in cooperation with strong partners in EU and NATO member states, including through the development of defensive capabilities, in conjunction with the needs to defend the national territory;
- Actively promoting the concept of Smart Defence at the level of the Western Balkans and in the eastern neighbourhood of Romania, including through the development of capabilities that can have customers on the regional profile market. In an area characterised by increased nationalistic sentiment and exacerbation of nationalistic egos, such an initiative of Romania would help to strengthen the strategic profile of our country as a serious and credible partner, including at NATO and EU level;
- Development of strategic partnerships with the neighbouring countries of Romania (e.g. Western Balkans, Ukraine, Republic of Moldova), for the purpose of producing and marketing military products for this emerging market, while increasing the degree of security at regional level, including by accessing the EU non-refundable funds;
- Achieving/consolidating partnerships with countries in the Middle East and Asia region, which have important resources to purchase modern combat technology, given the positive image of our country in these regions

where there were, prior to 1989, consistent partnerships that concerned the delivery of weapons;
- Constant participation of companies in the domestic defence industry at the main international trade fairs and exhibitions, in order to diversify the portfolio of customers and to penetrate the profile markets in expansion.

A special opportunity for the Romanian profile industry is the European Defence Fund, which will promote defence capabilities in EU member states, and in this context the published 9 offer calls for the year 2019 and 12 calls for 2020, covering priority areas in all areas (air, land, sea, cyber and space).

For example, 80 million EUR are committed to facilitating the operations, protection and mobility of military forces (e.g. development of CBRN detection capacities and drone systems). Another 182 million EUR will be allocated to analyse the situation regarding the cyber sector and defence, 71 million EUR to support the modernisation of the next generation targets for target-impacting, 27 million EUR to support solutions on Artificial Intelligence, virtual reality and cyber technology, 100 million EUR to develop the Eurodrone project – a very important project for European defence autonomy and 37 million EUR to support the project ESSOR on secure and interoperable military communications.

In order to obtain relevant funding from this European funding mechanism, the Romanian defence industry must adapt swiftly to cover these relevant areas. From the analysis of the structure of the Romanian defence industry, it is critical to conclude partnerships with relevant actors on the international market, considering the lack of expertise in certain areas of activity.

The European Defence Fund focuses its financial efforts to develop comprehensive instruments and mechanisms for the *"war of the future"*, characterised by non-kinetic, hybrid actions and involving performance products and technologies.

PROPOSALS FOR MEASURES AT NATIONAL LEVEL

In the opinion of The New Strategy Centre, in order to achieve the development of the Romanian defence industry, proactive measures are needed at national level, which are to be supported by those arranged at international level, namely:

- *"Carrying out a comprehensive assessment of the indigenous defence industry for the purposes of privatization of state-owned security industry companies, including by merging companies with the same activity profile (e.g. 2016 – merger companies in Făgăraş and Victoria by carrying out a single entity for the production of powders and explosives);*
- *Analysis of the opportunity to shift into the MoD coordination the undertakings which the state deems necessary to maintain under its control. The main*

argument in favour of this solution lies in the fact that this institution is the main beneficiary of the defence industry;

- *Elimination of duplication of arms export arrangements, given that in many situations, ROMARM and ROMTEHNICA competed in order to obtain contracts on the external market and their winner was a third-party company in another state;*
- *To develop consistent investment programmes in the field of research and development, including through strengthening cooperation between the institutions within the national security system and state and private companies operating in this domain;*
- *Conceptualising and developing a national defence research and development programme, while updating the legislative framework to enable private investment in research and development, with the guarantee that the result, validated in the specific tests, will lead to national projects financed by the state;*
- *The development of public-private partnerships with partners of the defence industry in the country and abroad, from NATO and EU countries, as well as the creation of the conditions necessary for the deployment of advantageous offset contracts in the military technique acquisition/modernisation;*
- *Consistent investment in dual-use capabilities – civil and military;*
- *Adopting a policy to impose common technological standards in production, research-development and procurement activities;*
- *Set up a cyber defence entity to act coherently and integrated in response to cyber-related aggression on national critical or military-type infrastructure elements".*

CONCLUSIONS

In the coming period, the Romanian defence industry has tremendous development potential, given the geostrategic position in NATO's south-eastern flank. At the same time, the indigenous defence industry is well known in certain emerging markets, and it is possible to increase exports in some countries that have financial potential.

Considering certain restrictions on the export of military products and technologies, it is necessary to take certain measures to comply with all international treaties in the field of exports of military products and technologies, including the embargo regime. Romania is a member state of the Wassenaar Arrangement and complies with all the EU regulations in the field of export control of military products and technologies, being a regional leader in this field.

The Romanian defence industry faces systemic problems, which do not allow the development of this particularly sensitive sector to reach its real potential. In this context, it is necessary to invest consistently in the research and development sector, while extending strategic partnerships with relevant companies in the Euro-Atlantic area, the Romanian profile industry thus assimilating modern technologies.

Moreover, an important factor is the acquisition of weapons and military equipment by the Romanian Armed Forces, currently the degree of absorption being about 10%, well below the average at the level of the European Union member states (70%). The acquisition process of the Romanian Armed Forces must consider the new threats coming from the east, including those of a hybrid nature.

WEBOGRAPHY

1. www.ancex.ro.
2. https://www.fonduri-structurale.ro/stiri/21714/se-urmareste-realizarea-unui-centru-de-cercetari-al-industriei-de-aparare-inclusiv-prin-accesare-de-fonduri-europene;
3. https://www.investingromania.com/ro/stiri/stiri-agerpres/b-d-l-u-industria-de-aparare-are-de-10-ori-bugetul-de-execu-ie-de-anul-trecut;
4. https://www.libertatea.ro/stiri/sindicalistii-din-industria-de-aparare-au-mers-la-cotroceni-2559266;
5. https://newstrategycenter.ro/wp-content/uploads/2016/04/2017-Martie-Ap%C4%83rare-%C8%99i-Industrie-studiu-New-Strategy-Center.pdf.

IMPLICATIONS OF UTILISING UNSCR 1325 "WOMEN, PEACE AND SECURITY" AGENDA FOR THE CONDUCT OF INTERNATIONAL MILITARY OPERATIONS AND MISSIONS IN THE CONTEXT OF THE NEW SECURITY PARADIGM

Silvia STANCIU

PhD Candidate, "Carol I" National Defence University, Bucharest

UN, NATO and EU member states have substantially contributed, in the last 20 years, various resources, to the initiatives that have been assumed in accordance with the provisions set by the international cooperation developed regarding gender perspective promotion, especially in the context of armed conflicts. Normative frameworks together with the working mechanisms that have been adopted and developed in this domain, establish high standards for UNSCR 1325 agenda implementation, with notable references regarding security and defence, this being a field of expertise and activity which is directly and permanently influenced by the manner in which armed troops exploit, in the conduct of their military operations and missions, the new set of operational perspectives, introduced to them by taking into consideration the gender dimension. In the context of the new security paradigm, the vision upon the global architecture of risks and vulnerabilities imposes the adoption of punctual and equally robust measures in order to counteract any emergent risks that lay an immense pressure upon general safety and progress.

In essence, international security organizations subscribe that gender diversity may be a strength trait in favour of societal reconciliation and rehabilitation, by utilizing the military component as a cardinal vector in putting UNSCR 1325 "Women, Peace and Security" objectives into practice. Therewith, the dynamics and the complexity of modern conflicts have validated the importance of conceiving the security policies as promoters of social equality and inclusion, all these representing essential conditions for acquiring international peace.

Keywords: gender perspective, UNSCR 1325, security paradigm, gender diversity, inclusion.

INTRODUCTION

Contemporary armed conflicts have revealed, through their evolution as well as through their specific way of manifestation, the importance of approaching gender issues in a comprehensive manner, especially in regards to the security and defence domain. Gender inequality often precedes and is exacerbated by conflicts, which means that including gender perspectives in the preparation and conduct of missions, military operations, and also in peace negotiations, is an essential resource for establishing peace anywhere in the world.

UN, NATO and EU member states have invested, in the last 20 years, considerable time, finances and human resources within the initiatives undertaken in line with international cooperation in the field of promoting gender perspective through the UNSCR 1325 agenda *"Women, Peace and Security"*. Consequently, for the implementation of the four pillars of reference in the field, *prevention, protection, participation, and humanitarian assistance and recovery*[1], policies, strategies and action plans have been developed by mixed groups of experts, with the aim of providing a common line of gender perspective integration with celerity and responsibility within the planning, execution and evaluation activities. Recent military operations, as well as the current ones, include a gender analysis meant to actively contribute to the integration of the new perspectives that objectively mirror the differences between men and women as they are highlighted in the roles and the social interactions of people, in the distribution of power and in the level of access to resources[2].

The new security and defence paradigm is closely connected to the increasingly unpredictable dynamics of the security environment[3], and it is the result of a complex, constantly changing, architecture of risks. In this context, the gender dimension offers to the security structures, and implicitly the armed forces, a new perspective of addressing these risks centred on the individual and the society he/she belongs to, in order to ensure gender equality and to eliminate all forms of discrimination and violence against women. This new type of approach,

[1] United States Institute for Peace, *What Is UNSCR 1325? An Explanation of the Landmark Resolution on Women, Peace and Security*, https://www.usip.org/gender_peacebuilding/about_UNSCR_1325, retrieved on 10.09.2019.

[2] Helene Lackenbauer, Richard Langlais, *Review of the Practical Implications of UNSCR 1325 for the Conduct of NATO-led Operations and Missions*, NCGM, 2013, p. 25.

[3] Presidential Administration, *The National Defence Strategy for the 2015-2019 Period, A Strong Romania in Europe and Worldwide*, București, 2015, p. 5.

largely imposed due to the volatility of the hybrid and asymmetrical threats that humanity has to face, has implicitly dictated a reform of the security providing structures, which, although considered to be of men's expertise, have adapted to the environmental requirements by transforming gender diversity into a capability, used to increase organizational performance.

UNSCR 1325 *"WOMEN, PEACE AND SECURITY"* AGENDA IN THE CONTEXT OF THE NEW SECURITY PARADIGM

Resolution 1325 is one of the most important and inspired achievements of the United Nations Security Council, crowned by the global movement, in full progress, of empowering and valorising women in all social and professional domains. The last 20 years have been profoundly marked by the international actions developed in order to guarantee gender equality, this being classified as a human right, cardinal to establishing peace and sustainable development, by using in this sense, the full available human potential[4].

The contemporary risks management has been redefined due to the changes inserted within the security paradigm. Thus, the unique ways of manifesting them have largely led to the advancement of the gender agenda, which may be an effective solution for combating risks by using the most efficient and resilient existing resource, respectively the human resource. Practically, security providing structures, especially the armed forces, have resorted in the last quarter of the century to strategies meant to eliminate the existing barriers regarding the admission, promotion and maintenance of women in the military systems. The demands associated to the modern operations environment, in which the social and the cultural components have an extremely important significance, emphasise as being a true asset the opportunity of jointly exploiting the skills of both male and female military personnel[5].

The latest report of the World Economic Forum on the prevalence of global risks associated with 2019 brings to the fore the social divides as having an increased potential for generating armed conflicts. By promoting the hypothesis that there is a human side to every global risk[6], the analysts have demonstrated that the lack of respect for human rights and the prevalence of prejudices and stereotypes related to individuals or groups of people, lead to social vulnerability and amplify

[4] United Nations, *Global Issues, Gender Equality,* https://www.un.org/en/sections/issues-depth/gender-equality/, retrieved on 12.09.2019.

[5] North Atlantic Treaty Organization, *Gender Perspectives in NATO Armed Forces*, 2019, https://www.nato.int/cps/en/natohq/topics_101372.htm, retrieved on 12.09.2019.

[6] World Economic Forum, *The Global Risks Report 2019*, 14th Edition, Geneva, 2019, pp. 5-9, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, retrieved on 12.09.2019.

both the incidence and the impact of complex risks. In this regard, the international community has made extended efforts to integrate the gender perspective in the field of security and defence, thus ensuring that all the initiatives carried on in this area involve and are equally addressed to women.

Currently, women occupy both leadership and executive positions in the armed forces that are deployed in international missions under the aegis of UN, NATO or EU. However, due to the specific nature of the missions (non-combat, training and advise), the arrangements established for the mission (tactical team, platoon), the geographical layout of the theatres of operations (Afghanistan, Kosovo, Iraq, the Mediterranean) as well as due to the shorter dislocation time (6 months – maximum 9 months) the number of women present in NATO[7] military missions is constantly higher than in UN[8] or EU[9] missions. Although the attitude in the selections made for such positions is constantly proactive in the sense of them being occupied by women, the female military personnel are often reluctant, their decision being strongly influenced by the important role played by them in the family, especially as mothers. For these reasons, statistics on participation in military operations and missions still reflect a large discrepancy between the number of women and men deployed in the theatres of operations.

However, at the level of the armed forces belonging to UN, NATO and EU member states, the principle of gender equality is respected, by both applying equal standards of admission within the military system and providing equal rights, responsibilities and opportunities for accessing all military branches and positions no matter the hierarchical level. In this regard, the universally accepted standard is that of human resource performance, this being the only one capable of keeping the operational demand and supply balance during the evolution of the military actions, regardless of the associated risk. The UNSCR 1325 agenda is set up in a common reference point for gender issues and offers a high-performance legislative framework, constantly adapting and transforming, which is essentially necessary for the implementation of the gender axis. At the same time, it facilitates the establishment of widely accepted and implemented working mechanisms such as the committees, the political and military structures of expertise in the field, the task force, the special representatives appointed to occupy permanent or dual-hatted positions related to counselling on gender-related issues[10].

[7] North Atlantic Treaty Organization, *Operations and Missions: Past and Present, Current Operations and Missions,* https://www.nato.int/cps/en/natohq/topics_52060.htm, retrieved on 12.09.2019.

[8] United Nations Peacekeeping, *Chart on the Number of Male and Female Uniformed Personnel Working across UN Missions (31 July 2019)*, https://peacekeeping.un.org/en/gender, retrieved on 12.09.2019.

[9] European Union external Action, *Chart on Military and Civilian Missions and Operations*, https://eeas.europa.eu/headquarters/headquarters-homepage/430/military-and-civilian-missions-and-operations_en, retrieved on 12.09.2019.

[10] Helene Lackenbauer, Richard Langlais, *Review of the Practical Implications of UNSCR 1325 for the Conduct of NATO-led Operations and Missions*, NCGM, 2013, p. 29.

THE IMPLICATIONS OF USING UNSCR 1325 *"WOMEN, PEACE AND SECURITY"* FOR THE CONDUCT OF MILITARY MISSIONS AND OPERATIONS

Depending on the specifics of each theatre of operations and military mission, as well as on the actors involved, the conflict-gender nexus can be assigned to various forms of manifestation, whose main stake is security. The prevalence of armed conflicts often leads to insecurity, reducing on the one hand, in the case of women, their space and opportunities for life, and on the other hand increasing their vulnerability and the need to be protected[11]. For this reason, poverty and social vulnerability are two major factors in widening the recruitment pool for insurgent groups and organized crime[12], women being a potential direct or indirect actor involved in armed confrontations, ensuring an immense moral and logistical support[13]. Thus, not only the role and participation of women in society but also the level of respect for their rights are central elements of the gender analysis carried out in order to conduct military operations under the auspices of the international law on combating gender discrimination and the elimination of all forms of violence against women.

Due to the dynamics and the complexity of the current conflicts, military components are pretended to be a cardinal vector of operating the objectives set out in the UNSCR 1325 agenda *"Women, Peace and Security"*, transposing the concept of gender diversity into a special capability assigned to the structures that are externally deployed. Assuming this capability by the armed forces dictated not only the reorganization of the combat structures but also the reform of the planning and training elements, in the sense of recognizing and exploiting the potential of the gender coordinate within the conflict resolution.

At present, the debates on women's participation in international missions and operations are no longer limited to the UN alone, as they are a central item on the discussions' agenda of all security providing organizations, including NATO and the EU, demonstrating a huge interest on the subject as well as the fact that gender has a cardinal importance in the fight against complex risks and for peace guaranteeing.

[11] Bjorn Holmberg, *Strategic Conflict Analysis of Afghanistan - 4.3.5 Vulnerable and Potentially Powerful Actors*, swede.peace/SIDA, reference number 2011-000560, Stockholm, 2012, p. 18, http://swedepeace.org/wp-content/uploads/2013/07/Strategic-Conflict-Analysis-Afghanistan-FINAL-PUBLISHED-January-19-2012-COMPRESSED.pdf, retrieved on 13.09.2019.

[12] *Ibidem*, III.

[13] Helené Lackenbauer, David Harriman, *Women at the Peace Table: Rhetoric or Reality?*, Stockholm, 2013, p. 41, https://www.academia.edu/4774121/Women_at_the_Peace_Table_Rhetoric_or_Reality_Women_s_participation_and_influence_in_the_peace_and_reintegration_process_in_Afghanistan, retrieved on 13.09.2019.

MILITARY OPERATIONS CARRIED OUT UNDER THE AEGIS OF THE UN

The UN deployed troops, for the first time, in 1956 as part of its first armed peacekeeping operation established to manage the Suez Chanel crisis. Until the end of the Cold War, peacekeeping operations consisted largely of classical military operations, carried out with light infantry armament, these being, essentially, from the perspective of participation, dominated by men. Since 2006, the UN has carried out a substantial number of missions throughout the world, especially on the African mainland, often opting, in favour of efficiency, for a military mandate (for observing how ceasefire agreements are applied or for monitoring the withdrawal of the combatants from the conflict zones) as well as for a civil one (strengthening the rule of law and building peace) within the same operation.

Statistics[14] drafted on the theme that is associated with the UNSCR 1325 agenda show that the tendency was to have a very low number of women accessing UN missions at the level of military structures in comparison to the civilian or police structures. Thus, if in 1993 only 1% of the military personnel deployed in UN operations were women, today, out of the total of 90,000[15] uniformed personnel, 3% are women from the military background and 10% are women belonging to the police forces.

During the missions, the female military personnel are assigned to locally contribute, by their own example, to the empowerment of women and girls, often in a male dominated society, to support women from host communities in their struggle for their own rights and for their active involvement in all peace processes.

In this regard, the recruitment of a higher number of women[16], especially those who are trained for advancing the gender agenda, for the UN military missions' development has the following direct implications:

- Empowering women within the host community;
- Addressing the specific needs of ex-combatant women during the process of demobilization and reintegration into the civilian life;
- Facilitating access for women from host community to the peacekeeping force by making it much more accessible;
- Facilitating access to victims of gender-based violence;
- Counselling female cadets from the host nation's military academies;

[14] United Nations Peacekeeping, *Women in Peacekeeping – Chart*, https://peacekeeping.un.org/en/women-peacekeeping, retrieved on 15.09.2019.

[15] United Nations Peacekeeping, *Gender, Troops July 2019 – Chart*, https://peacekeeping.un.org/en/gender, retrieved on 13.09.2019.

[16] United Nations Peacekeeping**,** *Why Is It Important to Have Female Peacekeepers?*, https://peacekeeping.un.org/en/gender, retrieved on 13.09.2019.

- Facilitating full access to members of the host nation, including women who are prohibited from talking to men due to their social traditions.

At the same time, the involvement of female military personnel within the peacekeeping missions represents an adapted way of reducing confrontations and resizing conflicts, used to improve the support given to women from local communities, additionally giving perspective through alive and present image of female role models and of course broadening the spectrum of qualifications available in peacekeeping missions. Through this, the level of local security increases, the population, as a whole, benefits from the presence of and the action taken within the host nation, by the international troops.

The UN currently has the highest number of gender enablers responsible for strengthening, coordinating and developing the skills needed for the integration of gender equality into humanitarian actions, being them generated by both armed conflict and natural disasters. In this regard, *UN Women* is the main organization initiated by the UN relating to promoting gender capacity in missions attached to conflict countries as well as to promoting the "*Women, Peace and Security"* agenda at a global and national level.

NATO – A LEADING ORGANIZATION IN THE FIELD OF PROMOTING WOMEN FOR HIGHER RATES OF PARTICIPATION WITHIN THEATRES OF OPERATIONS

The year 2007 constitutes at the level of the North-Atlantic Alliance the reference year regarding the initiation in the gender issue working domain through the adoption and the development of the EAPC (NATO/Euro-Atlantic Partnership Council) Policy for the implementation of UNSCR 1325. Although the Policy reinforces the necessity of increasing the number of military women deployed in theatres of operations, the implementation of this exact aspect falls, in order to obtain gender balanced NATO forces, within the responsibility of each member state. The efforts made in this regard are annually reported by the member states, these data composing the basis for any statistics regarding the integration of the gender perspective within the member states' military structures as well as in the operations and missions carried out under the NATO umbrella.

A thoughtful study of the NATO annual reports on the gender theme attests that, almost 20 years after the adoption of UNSCR 1325, women[17] continue to access in a lower percentage positions available within the international missions. The main

[17] Theodora-Ismene Gizelis, Louise Olsson, *Gender, Peace and Security – Women in International Operations*, Routlege, New York, 2016, p. 43.

reason generating this situation lies in the direct proportionality existing between the participation of women in the armed forces of the NATO member states and their participation within the international missions. However, at the national level, considerable efforts have been made throughout the entire Alliance, in order to reform the human resources policies so as to eliminate the differentiated scales of admission set for the military education and training institutions, as well as to facilitate access for women to the full spectrum of military branches, including those related to close combat.

Being the organization with the largest number of military women that choose to be deployed in foreign missions, NATO has become a true hub for promoting the gender perspective on a large scale. Thus, within the operations carried out, especially in Afghanistan, a series of facilitators were developed which, although initially established as force protection measures, were later noted as real capabilities, massively contributing to the successful completion of the military tasks regarding the engagement of the entire host nation in the processes of restoring security and guaranteeing peace. The further facilitators have been used, in order to provide a broader picture of the area of responsibility, in multiple tactical situations as follows[18]:

- Female Engagement Teams (FETs) – mixed teams of military or civilian women, whose purpose is to identify within the local society the specific needs of women and girls and gather information on the current situation of local communities, including aspects referring to insurgent activities, in order to potentiate military decisions in the planning phase of operations in the area;
- Cultural Support Teams (CST) – teams used to incorporate the gender perspective in the special operations; they have been used in stability operations during three phases, namely security, governance and development;
- Foreign Area Specialists – specialists associated with information, communication and psychological operations, responsible for engaging influential women from the operations area, with the purpose of accessing networks and decision-making mechanisms on cultural issues, from a gender sensitive perspective;
- • Liaison and Monitoring Teams (LMT) – teams having the ability to access local communities and the potential to introduce the gender perspective at the level of all interactions taking place with the representatives of the local communities;

[18] Helene Lackenbauer, Richard Langlais, *Review of the Practical Implications of UNSCR 1325 for the Conduct of NATO-led Operations and Missions*, NCGM, 2013, pp. 29, 37, 56.

- Gender Focal Point (GFP) – staff trained in the field of gender, appointed on a voluntary basis to disseminate and contribute to the implementation of the gender perspective in the military operations;
- Gender Adviser (GENAD) – staff trained in the study of gender issues that ensures the integration and understanding of UNSCR 1325 and the gender dimension within all levels of the military commands of different components – land, air and naval – by offering advice or giving practical support for the implementation of the gender perspective in NATO operations and missions; this position is a permanent one;
- NATO Special Representative on Women, Peace and Security – a permanent position held by a senior diplomat, within the NATO Headquarters, having the role of coordinating civil-military working groups on the implementation of gender policies.

Acquiring the lessons identified and learned within the theatres of operations has substantially contributed to the Alliance's adaptation to the context of contemporary conflict unfolding. NATO has thus succeeded in increasing the level of understanding and awareness of its troops regarding the importance of involving women in the field of security and defence, which has led to a reform of the entire system regarding recruiting, teaching and training of troops, and also to an evolution of the human resources management during the missions.

THE STATUS DESCRIBING THE LEVEL OF FEMALE PARTICIPATION WITHIN EU'S FOREIGN MISSIONS

In 2003, the EU launched its first international peace mission, with personnel assigned from the police structures, in Bosnia and Herzegovina. Since then, the EU has implemented the Common Security and Defence Policy under the auspices of which it has deployed staff in over 30 other military and civilian missions. In 2005 the first EU Policy was adopted and it explicitly addressed the need to increase the number of women participating in the organization's external missions, globally operated, but somewhat concentrated in certain geographical areas of EU relevance. The immediate next step was to collect gender segregated data on the personnel deployed in foreign missions all this being made without making any differences between the civilian and the military staff[19]. This measure represented, in the first phase, a way of emphasizing at the level of international activities the manner the EU has chosen to promote the gender agenda. With the further implementation of UNSCR 1325, at the level of civilian missions mandated to strengthen the rule

[19] *Ibidem*, p. 51.

of law, to contribute to peace building and to monitor human rights enforcement, it has been observed a steady increase in the number of women participating to field operations. The statistics also show a general increase in the number of women from all categories opting to be assigned in operations developed under the EU aegis. A determinant factor of this conjuncture, beyond the implementation of gender sensitive policies, is also the low level of potential risk specific to EU missions, civilian and military personnel prevalently choosing those operations that are carried out in areas where the intensity of conflicts is decreased[20].

The EU Strategic Engagement on gender equality, adopted for 2016-2019, is a legal and conceptual tool of EU used to translate into practice, in any present and future activities, the full implementation of gender equality. The Engagement is focused on five key, EU specific, areas of action[21], applicable to international missions developed under this organization' umbrella:

- Increasing female labour market participation and economic independence of women and men;
- Reducing the gaps between men and women in terms of payment, earnings and pensions, as well as in relation to working and retirement conditions; the fight against poverty associated with the proliferation of gender stereotypes;
- Promoting equality between women and men in decision-making;
- Combating gender-based violence, protecting and supporting the victims;
- Promote gender equality and women's rights throughout the world.

This commitment reaffirms the organizational will expressed towards the integration of the gender agenda, the perspective associated with this field being included in all policies, financing programmes, actions and activities carried out by the EU.

CONCLUSIONS

International security providers such as UN, NATO and EU are the main source of promoting and implementing the gender agenda, at all levels, from tactical to strategic, in spite of the typology of operations or missions to be carried out. These organizations have understood that beyond the stereotypes associated with each gender, there is an extensive pool of talented people, able to perform within international missions, under the conditions and the pace imposed by the fight against any emerging risk, regardless of its source and complexity.

[20] *Ibidem.*

[21] European Commission, *Gender Equality Strategy – Achievements and Key Areas for Action*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/gender-equality-strategy_en, retrieved on 16.09.2019.

Introducing the gender perspective within security and defence domain, in the context of the new security paradigm, represents the tangible expression of the fact that sustainable peace demands a comprehensive approach of the social environment, women, men and children being involved and engaged, on a mandatory basis, in the processes regarding security and conflict resolution. At present, the interdependence between the integration of the gender perspective and the increase of the operational effect of the missions is evident. The failure to manage the gender dimension at the social level is also a major impediment to the achievement of the operational objectives set at the political or military level.

The implementation of the gender perspective is a complex process, which involves special qualifications, acquired and practiced in specific training sessions, and applied in the military missions and operations carried out in various areas around the globe. The existence of standardized positions or structures that ensure the integration of the UNSCR 1325 agenda in the military operations is an essential clause for guaranteeing objectivity in the design and execution of gender analysis at the highest level of performance, in order to use it effectively in the planning and conduct of military missions.

The current architecture of contemporary risks and threats reaffirms the need to use the full range of available resources, especially the human resource, its diversity being an intelligent way of approaching the fight against terrorism, radicalization, trafficking generated by the organized crime networks, or to diminish the negative effects of the natural disasters, respectively a way to deal with all threats of hybrid, unconventional nature. In this respect, promoting equality and inclusion on all levels is a precondition for social reconciliation and conflict resolution, regardless of their specific nature.

The 21st century constantly reflects the reality that determined security and defence to become a domain of collective responsibility. Modern armed forces, part of global alliances, have long started to lead the way with their innovative approaches to all aspects of diversity and employment equity, one major change being the unilateral acceptance of women within the combat branches and decision-making positions. Thus, fully integrating and valuing women inside the military organizations have enriched the military portfolio of capabilities and supplemented the ability of the forces to be globally deployed in complex missions where the operationalization of gender perspective is compulsory for increasing security and mission effectiveness.

BIBLIOGRAPHY

1. ***, *NATO Annual National Reports*, https://www.nato.int
2. ***, North Atlantic Treaty Organization, *NATO/EAPC Policy on Women, Peace and Security*, Brussels, 2018.
3. ***, North Atlantic Treaty Organization, *Bi-SC Directive 40-1 – Integrating UNSCR 1325 and Gender Perspectives in the NATO Command Structure*, Brussels, 2017.
4. ***, North Atlantic Treaty Organization, *Summary of the National Reports of NATO Member and Partner Nations to the NATO Committee on Gender Perspectives*, Brussels, 2016.
5. ***, North Atlantic Treaty Organization, *Gender Perspectives in NATO Armed Forces*, 2019.
6. ***, European Commission, *Strategic Engagement for Gender Equality 2016-2019.*
7. ***, Presidential Administration, *The National Defence Strategy for the 2015-2019 Period, A Strong Romania in Europe and Worldwide*, București, 2015.
8. ***, United Nations, *Global Issues, Gender Equality.*
9. ***, North Atlantic Treaty Organization, *Operations and Missions: Past and Present, Current Operations and Missions*, 2019.
10. ***, World Economic Forum, *The Global Risks Report 2019*, 14th Edition, Geneva, 2019.
11. ***, United States Institute for Peace, *What Is UNSCR 1325? An Explanation of the Landmark Resolution on Women, Peace and Security*.
12. ***, United Nations Peacekeeping, *Why Is It Important to Have Female Peacekeepers?*, 2018.
13. ***, United Nations Peacekeeping, *Chart on the Number of Male and Female Uniformed Personnel Working across UN Missions*, 2019.
14. ***, European Union External Action, *Chart on Military and Civilian Missions and Operations*, 2019.
15. ***, United Nations Peacekeeping, *Women in Peacekeeping – Chart*, 2019.
16. ***, United Nations Peacekeeping, *Gender, Troops, July 2019 – Chart*, 2019.
17. Carol Cohn, *Women and Wars*, Polity Press, London, 2018.
18. Theodora-Ismene Gizelis, Louise Olsson, *Gender, Peace and Security – Implementing UN Security Council Resolution 1325*, New York, Routledge, 2016.
19. Bjorn Holmberg, *Strategic Conflict Analysis of Afghanistan Stockholm*, 2012.
20. Helene Lackenbauer, Richard Langlais, *Review of the Practical Implications of UNSCR 1325 for the Conduct of NATO-led Operations and Missions*, Brussels, 2013.
21. Helene Lackenbauer, David Harriman, *Women at the Peace Table: Rhetoric or Reality?*, Swedish Ministry of Foreign Affairs, Stockholm, 2013.
22. Laura Sjoberg, *Gender, War and Conflict*, Polity Press, London, 2014.

IMPROVING PERFORMANCE AND RISK MANAGEMENT IN PROCUREMENT BY DEVELOPING A COMMON PLATFORM AT THE MINISTRY OF NATIONAL DEFENCE

Alexandra-Ioana MARIAN
Land Forces, Bucharest

The procurement performance translates in terms of effectively managing public funds through the acquisition of products that meet customers' requirements, are delivered on time, and under advantageous conditions.

A systematic analysis of the legislative barriers and factors that influence procurement offers a clear image of the vulnerabilities associated with implementing the process. By applying modern risk assessment methods, an information package can be designed to support the decision-making process of how to effectively allocate resources in order to achieve the performance objectives established.

This paper offers a practical solution for improving procurement performance by developing a common platform, at the Ministry level, where the results obtained by each contracting authority are analysed objectively and transparently. The platform also offers support in planning an acquisition, serving as aid to all contracting authorities that engage in such activities.

Keywords: performance management, life cycle, RSAP (Resources and Support for Public Acquisition) platform, risk management.

INTRODUCTION

While new-generation equipment is becoming increasingly complex and the performance has been improved, supply management turns out to be extremely valuable and it is considered to be the primary component of organizational management; it must therefore exist a permanent balance between the required equipment and the available amount of goods that can be provided by a supplier. In practical terms, the main function of the supply process is to provide the total amount of goods and equipment, at the place and time required, under the most advantageous conditions.

The missions and objectives during peacetime are directly related to the defence capabilities of each military unit, and a fair analysis of the main constraints determined by using at the same time a large number of outdated equipment (incompatible with NATO defence systems) and a wide range of new equipment that has been recently acquired, along with a low-performance maintenance system (caused by insufficient or non-conforming spare parts and materials along with non-specialized personnel or too many tasks that should be performed at the same time) allow the decision-makers to optimize their decisions taking into account the best resource management strategies.

There are specific procedures for the supply with military equipment as well as with consumer goods. It may be used either a Foreign Military Sales (FMS) programme or an in-country acquisition plan, according to the competencies granted and in compliance with the Romanian legislation regarding the spending of public funds.

In this paper I will analyse the constraints that influence the performance of public procurement in the military organizations and I will present a framework for improving communication within and outside organization, along with using modern techniques for risk identification and assessment, such as *Brainstorming* or *Delphi Method*[1].

Information management in similar structures can be improved by developing an application, for the Ministry of National Defence or for particular types of military forces, which has two main functions:

- it allows access to a database where you can find information regarding procured goods, technical documentation or award documents, examples of agreements, product reviews during lifetime and other helpful information;

[1] SR EN 31010:2011, *Risk Management. Risk Assessment Techniques.*

- it is a useful instrument for online communication, in real time or through messages, which allows the exchange of ideas or opinions between the requester and any of the other members able to provide solutions, very useful in analysing and managing the risks associated with the procedure.

The functions of the platform, the way it is used and the interaction between the operators registered in the system are represented by an easy-to-use graphical interface which is highly upgradeable and new functions will be continuously added.

Contract performance management and risk management in procurement are elements that directly strive with the fulfilment of logistical objectives, where the supply management is integrated in the organizational management and adapted according to the established strategies.

RISK MANAGEMENT IN THE PROCUREMENT OF MILITARY SUPPORT EQUIPMENT

A mission can be accomplished only if logistic support is provided on time and according to the requirements.

In supply management, and especially in the procurement system, the lack of specialized knowledge and the legislative fluctuations are the main barriers to achieving performance.

The relevant elements that can be considered as reference when we discuss about the performance of the procurement process are: the ability of the purchaser to conform to the procedure timetable and to spend all the funds allocated through the budget, the ANAP[2] validation of the award documentation, contracting goods in advantageous condition, as well as the lack of complaints and claims from bidders or regulators, while complying to a code of ethics in procurement.

The analysis of the procurement process performance provides an overview on the flow of activities and the level of satisfaction of the stakeholders, so that all the measures are adopted to improve the results of future procurement procedures.

In procurement, *"risk management"* includes all the activities necessary to identify and control the risks that may have an impact on the fulfilment of the terms and conditions of a contract. Within the military organizations, the activities are carefully organized and carried out under the command and supervision of an officer in charge, so that the main function of risk management is to ensure a global control of risks, which allows maintaining an acceptable level of risk exposure, with minimal costs.

[2] ANAP – *Agenția pentru Achiziții Publice* – a Romanian public institution, established under the authority of Ministry of Public Finance according to GEO no. 13/2015 on the establishment, organization and functioning of the National Agency for Public Procurement.

The main expectations and strategic objectives of the military institution regarding the risk management in procurement, along with the activities that contribute to the fulfilment of the proposed goals are:

- protecting public funds against fraud, violations of law and errors;
- ensuring efficient procurement management and according to the standards imposed by ANAP;
- ensuring that there are procedures for managing vulnerable situations with impact on objectives;
- providing an organizational framework that allows to carry out the activities in a controlled and efficient manner;
- improving the planning and decision-making processes, through a well-founded analysis of activities, weaknesses and strengths;
- responsible and substantiated allocation of human and financial resources in the direction of the designated strategic objectives;
- developing the skills and attitude of the employees, in order to increase the efficiency of the current activities and to face the challenges and crisis situations.

The fundamental objective of the procurement system is to efficiently manage the public funds in order to obtain *"value for money"* [3],while complying with all the legal regulations *(Figure no. 1)*.

While completing all the procedural stages of an acquisition, lots of constraints and dysfunctions are uncovered, with direct effects on the procedure schedule and the resources involved, especially in the form of exposure to the involuntary violation of the principles of public procurement. In the military units, these dysfunctions exist and are often encountered, either due to budgetary fluctuations and the obligation to complete the purchases by the end of the budget year, or due to faulty planning of objectives and lack of correlation with the available funds. Too many tasks that need to be simultaneously performed, numerous complaints from the bidders or the prolongation and cancellation of the procedures have direct effects on the performance of the purchases, doubled by the lack of experience and professional knowledge of the persons responsible for the procedure, while public procurement legislation is continually changing in account of aligning with the requirements of the European Union Directives regarding the improving of the efficiency of public procurement.

[3] *"Value for money"* – in relation to public spending, it implies a concern with economy, efficiency and effectiveness, according to Richard Glendinning, *The Concept of Value for Money,* International Journal of Public Sector Management, Vol. 1 No. 1, pp. 42-50, Buckingham, UK, 1988, https://www.emerald.com/insight/content/doi/10.1108/eb002926/full/html, retrieved on 18.09.2019.

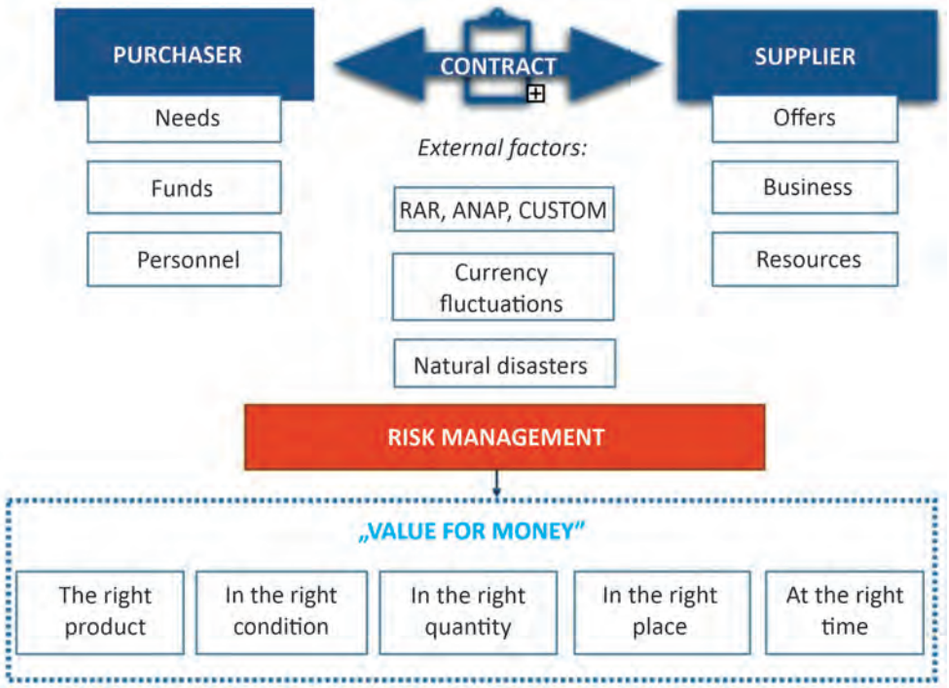


Figure no. 1: Risk management in procurement

CONCEPTUAL DEVELOPMENT OF A PLATFORM FOR RESOURCE MANAGEMENT AND SUPPORT FOR PUBLIC PROCUREMENT

Efficient resources management and impartial evaluation of procurement performance are facilitated by developing an application, for the Ministry of National Defence or for particular types of military forces, where the procurement results of each military organization are properly analysed; procurement specialists are going to fill in some questionnaires and the results will offer an overview of the procurement management in that particular military organization, with the purpose of permanent improvement of its activity.

To easily describe the process, the platform will be named *Resources and Support for Public Acquisitions (RSAP).* The platform is password-restricted and it contains a database with information about recently procured goods (breakdowns, warranty issues, reliability coefficient, or failure rate), available funds, ongoing or completed procurements, but also examples of System Requirements Documents, award documentation and contracts used by the organizations registered on the platform. Human resources are the most important asset – procurement specialists, end users and logistic organizations.

The steps are as follows: the purchasing organization is checking the database in order to verify if a similar product was procured in the past years. If the answer is affirmative, additional information can be provided, such as its availability or the System Requirements Document used for its procurement. These pieces of information are more helpful if the product is procured under the same circumstances and following the same regulations as now.

One can find information about the user of the product and can approach him to ask for details that can be useful in setting requirements, as well as information about related services (training, mandatory authorizations, logistic capabilities, and so on). Moreover, it can be accessed other purchaser database, in order to identify potential suppliers, estimated costs, requests for clarification or even observations submitted by other tenderers and challenges related to procurement procedures and contract management, as also key-practices for improving the performance of public procurement.

Accessing the database has no implications for members of the platform, the purchaser is fully responsible for planning and managing his own procurement; he has to identify all the risks related and to manage them properly in order to achieve the performance goals. Collecting ideas and identifying risks in the key moments, especially in the planning stage, could be done using *brainstorming* or *Delphi method*.

BRAINSTORMING

The concept of *brainstorming* was invented in 1938 by Alex Osborn and became popularized as a technique for collecting ideas and solutions to identified problems, an approach to managing risks and dealing with uncommon situations along with assessing risks, activities carried out by a skilled team who has information about the structure, the process or the programme that is going to be examined. The meeting should not last long, in order to remain focused [4].

The primary benefit of this technique is that the diversity of the group is significant, so the chances of discovering a brilliant idea are much higher than if the same group members would work individually. However, there are some disadvantages determined particularly by the inconsistency of the group and the pressure of finding the best solution in a short period of time, but also by external constraints on individuals, as each of them needs a certain amount of time to accommodate, and also the fact that extroverted people usually dominate the discussion, therefore introverted people hesitate to expose their ideas, which could be the good ones.

[4] Alex Faickney Osborn, *Applied Imagination: Principles and Procedures of Creative Problem Solving,* Charles Scribner's Sons, 3rd Edition, New York, 1963.

In this particular case, brainstorming can be applied through online videoconferencing, where the process is carried out according to the following plan: the military unit that plans to carry out a public procurement requests support to the RSAP administrator and asks for a meeting aimed at identifying the risks related to the planning of the procurement procedure. The RSAP administrator analyses the request and accesses the database with other military units that have made purchases of similar products. He also gets in contact with the Expert members[5].

The requestor may choose from the military units available on the platform and agree on the exact date for a meeting or, if it is urgent, a meeting will take place right away, but only with RSAP online members. The meeting will be moderated by the office responsible for the procurement, who will set out the topic of the meeting and the reasons for requesting it. It will be discussed the context of the acquisition, the identified risks, constraints on the closure date, the budget, certain market, organizational issues or the resources involved.

The requirements of the specifications and of the award documentation will be analysed and revised. The team is informed on the difficulties encountered during the acquisition planning, as well as the identified solutions. They pay particular attention to those situations that are subject to risks whose materialization may affect the achievement of the objectives.

Any of the participants can take part in the discussion in order to offer ideas or solutions based on the experience or good practices established in their own compartment. The discussion ends when the officer responsible for the procurement receives answers to all the questions submitted for discussion.

The aspects analysed and the solutions identified will be documented in a report of the meeting, approved by each participating member (using e-signatures) and submitted for approval to the manager of the requesting military unit. Subsequently, it is uploaded to RSAP, being automatically transferred to an online database, which offers punctual support to purchasers.

THE DELPHI METHOD

Although most often confused with the brainstorming technique, the defining feature of the Delphi technique is that the opinions on a particular subject are expressed individually and anonymously, and as the discussion progresses, the participants have access to the other answers, even having the possibility to change their mind about the previously expressed opinions.

[5] The contracting authorities receive scores according to the procurements carried out and their level of difficulty, but also according to the feedback received from other military units that have received support and advice from them as well as other relevant data. *Expert Level* – the highest rank in the hierarchy of contracting authorities

The method was first used in 1950 and has been developed since 1965 by Olaf Helmer within the Rand Corporation – a corporation founded by the United States Air Force, which brings together a group of experts whose opinions would be the basis for strategic decisions regarding the US defence industry and related to vulnerabilities towards the Soviet military power during the Cold War[6].

The Delphi method (which is also named *"the iterative investigation"*) is based on the principle that decisions from a structured group of individuals are more accurate than those from unstructured groups. Apart from the conventional Delphi, a *"real-time"* Delphi was developed, in which multiple survey rounds are temporally compressed to occur within a single meeting[7].

Some of the advantages are: overcoming the psychological barriers to expressing the opinion in a group, collecting a large amount of answers, thus the probability of finding viable solutions is very high, but also the fact that the participants do not have to meet simultaneously. On the other hand, the method has certain limitations determined by the involvement of a large number of specialists, as well as the time and efforts invested throughout the process.

Delphi investigation starts by setting the investigator and the theme of the meeting, also the major aspect on which the opinion of the specialists will be requested. A team of experts will be constituted and the first questionnaire will be formulated.

The second step consists in responding to the survey, submitting the answers to the investigator and improving the questionnaires based on the opinions expressed by the specialists. A particular aspect of this stage is that the surveys are going to be revised progressively, according to the opinions expressed by the members of the panel. The cycle is repeated until at least 80% of the group members have reached the consensus on the opinions inserted in the questionnaire.

The Delphi method can be used by a military unit who intends to carry out a procurement procedure, using the RSAP online platform and the same resources. The difference is that the questions will be submitted in a written form, using questionnaires/templates, summaries or any other methods chosen by the applicant; the RSAP administrator will analyse them and will send them individually to each member of the working group. Depending on the degree of complexity or the nature of the problem for which the investigation is requested, the questionnaires can be also submitted to the Expert level contracting authorities.

[6] Harold A. Linstone, Murray Turoff, *The Delphi Method. Techniques and Applications from the Foreword by Olaf Helmer*, https://www.yumpu.com/en/document/view/6822489/the-delphi-method-techniques-and-applications, retrieved on 18.09.2019.

[7] The differences between the conventional Delphi and Real-time Delphi are outlined on: https://intelligence.sri.ro/metode-de-analiza-delphi-si-real-time-delphi/, retrieved on 18.09.2019.

The investigator is the chief of the procurement department of the requesting unit, which has permanent access to the answers and can stop the process at any time, if the problem is considered solved. Otherwise, the formulation and completion of the questionnaires will be repeated until there is consensus among the members of the team.

Moreover, the Real-Time Delphi method can be applied through video conferencing, in which case only the online members will participate or, if the requesting military unit asks for specific specialists, the meeting will take place at a later date, depending on the availability of each participant.

The answers to the interviews are elaborated in real time, and the investigator can stimulate the discussion by inserting new questions or new issues/problems identified. The method not only supports the beneficiary in adopting the best decision, but it is also useful to the participants, due to exchanges of information and experience in similar fields.

Information processing and decision-making process are the final steps in conducting the Delphi investigation, the attention therefore moves to the processing, analysis and synthesis of the information obtained, the elaboration of the minutes of the meeting and the presentation of the results to the decision-makers, followed by the publication in the RSAP.

Integrating risk management into all procedural stages helps procurement managers to perform their duties on time and under the best conditions. Vulnerable situations are easily managed, and resources are appropriately allocated, through justified prioritization and even redistribution of tasks. The risks are managed efficiently by the persons in charge, who also have to anticipate in advance the vulnerabilities that can cause the interruption of the flow of activities, so that the best decisions can be taken to limit the negative effects.

A process approach to management provides an overview of the public procurement system and the factors that contribute to meeting the objectives, so that the contracting authority can adopt specific measures to minimize the risks, such as establishing advantageous contract terms and conditions, as well as optimizing the timing of the procedure in order to meet the expectations of the stakeholders.

RSAP INTERFACE DEVELOPMENT

The common Resources and Support for Public Acquisition (RSPA) platform comprises a database containing a high volume of information on the goods and materials purchased in recent years and information from the procurement file, as well as data related to the product life cycle.

The other function of the platform is real-time communication, online or through a messaging system, which allows the exchange of ideas or opinions between the applicant and any of the other members able to offer solutions, being a tool for identifying and analysing the risks related to the procurement procedure *(Figure no. 2)*.

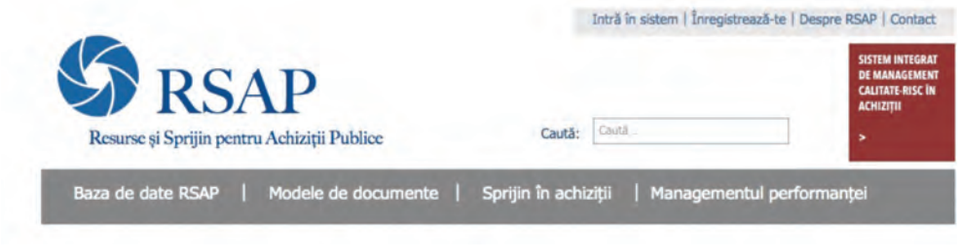


Figure no. 2: RSAP platform interface

The requesting military unit can find information about a certain category of products and their currently owners, who can be approached in order to provide information that can be useful for a proper elaboration of the technical specifications or for the establishment of the contractual terms.

Figure no. 3: RSAP platform interface – examples of documents

Moreover, following a specific product, one can verify information collected throughout its lifetime, from the moment it was purchased (technical specification, winning technical bid, offers of other potential suppliers, quality and warranty documents, user manuals, and so on), information regarding warranty claims,

preventive and corrective maintenance costs, information on the product condition at the moment (operable/non-operable), future prospects for its improvement or replacement *(Figure no. 3).* At the same time, the platform allows access to information regarding the analysis of product performance, which has been undertaken by the system based on the information entered by the user (MTBF, MTTR)[8] or the contract management (based on delivery time, non-compliant products, and so on).

Based on the information from the RSAP, the requesting military unit can identify additional risks beside the ones identified at the planning stage and it can discover other relevant factors that can influence the procurement procedure. For this reason, the risk analysis will be expanded accordingly. When the purchaser needs support, he issues a request to the RSAP administrator, who will analyse his request, and depending on the complexity or the nature of the problem, it will either specify the elements to be taken into account for an extended search on the platform or will access its own database (system administrator level) with contracting authorities that have made purchases of similar products or the Experts *(Figure no. 4)*.

Figure no. 4: RSAP platform interface – Support in acquisition

There are Entry-Level, Intermediate and Expert contracting authorities. The Experts have particular benefits such as participation in teambuilding activities with other Expert members or direct access to video conferences. Those are notable privileges that can be obtained and kept only under the conditions

[8] *MTBF – Mean Time Between Failures; MTTR – Mean Time To Repair*, http://www.armyacademy.ro/buletin/2_2004/a11.pdf , retrieved on 18.09.2019.

of active participation and providing relevant information during the meetings. The requesting military unit can get in touch with an Expert member to ask specific questions, but only if he is online and available.

The platform has one extra function – *performance management,* where a specialized procurement evaluation process uncovers the deficiencies of the system and the decision-making process, as well as the positive results obtained by some military units, successful acquisitions or even procurements that have exceeded all expectations (*Figure no. 5).*

The measurement of procurement performance in a particularly military unit can be made by setting up a meeting with the RSAP Expert members and without the presence of the parties involved in the contract (acquirer, end user, the evaluation committee, and so on) based on the results obtained and validated in the system (contract documents have been uploaded into the database immediately upon the completion of the acquisition). In such a way, the results obtained by each purchaser would be properly analysed.

Figure no. 5. RSAP platform interface – Performance management

Expert members are having wide experience in procurement and a great overview of the process, so they have no difficulty in foreseeing the results of the procedure, the expectations of the stakeholders and the influence of the internal and external factors, as well as the risks that should have been identified by the contracting authority and the strategy adopted for their management, in order to achieve the established performance objectives. Thus, an electronic survey will be developed and a series of questions will be asked separately and completed online, so that the results are instantly returned.

Following the analysis of all the documents resulting from the acquisition, the RSAP experts individually answer the questions from the survey then the results are validated and uploaded on the platform, where they can be consulted by the analysed military unit. The answers to the questions regarding the performance of the procurement system within a military unit highlight its ability to make sustainable purchases, the ability to manage critical situations and allocate resources, as well as the ability to use all the methods and techniques available to assess the risks that may influence the accomplishment of the objectives.

If there are reasons to believe that the results of the questionnaire do not reflect a correct image of the events and the results of the procedure, the analysed military unit may request a meeting with Expert members who have evaluated the performance of the procurement process, where they motivate their choices and offer support and advice to improving the procurement activity, in order to accomplish all the further performance objectives.

CONCLUSIONS

Military organizations fulfil their missions only with unconditional support from the logistic structures, which are responsible for the supply with equipment, goods and materials. For this reason, an effective procurement management is ensuring the quality of the product, their on-time delivery and in accordance with beneficiaries' expectations.

The use of modern techniques for risk identification and risk analysis could solve the problem of failing to meet the performance objectives in the procurement carried out by the military units, where the risks must be identified at an early stage, in order to be reduced to an acceptable level so as to be easily managed.

A collaborative management and a permanent interest in providing support to counterparts in the procurement structures of the Ministry of National Defence can bring multilateral benefits, in particular through the exchange of information on the good practices used by the purchasers and which have proven themselves the results, but also in terms of effective risk management and procurement efficiency.

The continuous improvement of the RSAP platform and the development of new functions allow it to become operational and very valuable, as it provides real-time information and specific data according to user's needs.

BIBLIOGRAPHY

1. ***, *Ghid ANAP în domeniul achizițiilor publice*, http://anap.gov.ro/web/ghiduri
2. ***, Law 98/2016 on Public Acquisitions (*updated), Methodology of law enforcement, approved by H.G. 395/2016.
3. ***, SR ISO 31000:2010 *Risk Management. Principles and Guidelines.*

4. ***, SR EN 31010:2011 *Risk Management. Risk Assessment Techniques.*
5. Susanne Baumann, Iris Erber, Magdalena Gattringer, *Selection of Risk Identification Instruments*, ACRN Oxford Journal of Finance and Risk Perspectives, Vol. 2, 2016, http://www.acrn-journals.eu/resources/jofrp0502c.pdf.
6. Richard Glendinning, *The Concept of Value for Money,* International Journal of Public Sector Management, Vol. 1 No.1, pp. 42-50, Buckingham, UK, 1988, https://www.emerald.com/insight/content/doi/10.1108/eb002926/full/html.
7. Olaf Helmer-Hirschberg, *Analysis of the Future: the Delphi Method, Report on RAND Corporation*, Santa Monica, March 1967, https://www.rand.org/content/dam/rand/pubs/papers/2008/P3558.pdf.
8. Harold A. Linstone, Murray Turoff, *The Delphi Method. Techniques and Applications from the Foreword by Olaf Helmer*, https://www.yumpu.com/en/document/view/6822489/the-delphi-method-techniques-and-applications.
9. Gheorghe Minculete, *Managementul achizițiilor. Elemente de marketing*, Editura Universității Naționale de Apărare, București, 2005, https://www.academia.edu/9978396/GHEORGHE_MINCULETE_MANAGEMENTUL_ACHIZIŢIILOR.
10. Adrian Nour, *Perfecționarea activităților de conducere și execuție a mentenanței din logistica Forțelor Terestre în condițiile actualelor provocări militare globale*, Doctoral Thesis, Summary, Editura Universității Naționale de Apărare, București, 2018, https://www.unap.ro/DOCTORAT/Rezumat_teza_mai%202018/REZUMATUL%20TEZEI_NOUR%20_RO.pdf.
11. Alex F. Osborn, *Applied Imagination: Principles and Procedures of Creative Problem Solving,* Charles Scribner's Sons, 3rd Edition, New York, 1963.
12. https://intelligence.sri.ro/metode-de-analiza-delphi-si-real-time-delphi/
13. http://www.armyacademy.ro/buletin/2_2004/a11.pdf

REPRODUCTIVE LEADERSHIP
– THE DIFFERENCE BETWEEN "STRAIGHT AHEAD" AND "FAST FORWARD" –

Mihai DĂIESCU
Master Student, "Carol I" National Defence University, Bucharest

Radu PRIOTEASA
Master Student, "Carol I" National Defence University, Bucharest

Be it seen as a modern society need or just as a nowadays old dusty idea, leadership can actually make the difference in a military organization between "straight ahead" and "fast forward".

According to John C. Maxwell there are 5 levels of leadership: 1. Position leadership – people follow because they have to; 2. Permission leadership – people follow because they want to; 3. Production leadership – people follow because of what you have done for the organization; 4. People development leadership – people follow because of what you have done for them personally; 5. Pinnacle – people follow because of who you are and what you represent.

This article aims to emphasize the military organization need for leaders, especially for level 4 leaders. As the technological evolution travels around the world with speed light, so should the human resource development through leadership do.

Level 4 leaders have the ability to empower others. They use their position, relationships and productivity to invest in their followers and develop them, until those followers become leaders in their own right. The result turns out to be reproduction. Level 4 leaders have the ability to reproduce themselves.

Seen from an economical/profitable point of view, leadership fills the space between standard performance and continuing efficiency. How can we multiply leadership in less time so we can have it all over our military organization and keep up with technological development speed? The answer is simple again. Forming and using from abundance level 4 leaders in order to develop other leaders. They are the ones that can exponentially multiply and speed up our human resource development in a realistic pursuit of great performance.

Keywords: reproductive leadership, continuing development, VUCA environment, level 4 leader.

Motto:
"Before you are a leader, success is all about growing yourself. When you become a leader, success is all about growing others".
Jack Welch

INTRODUCTION

Even though it is supposed to be a literature article we have decided that we would have an analytical approach upon this subject, trying to assert, prove and justify that *"reproductive leadership"* has become a realistic need or a problem to be solved within the military organization system.

Seen from a logical point of view, first we will try to paint the initial situation that we are dealing with not before defining the problem already identified. Secondly, we will explain why we do need to have reproductive leadership within the military organization, how we should do it and what the tangible consequences of greatly managing this fast enough are. Last but not least we will underline some conclusions not before briefly discussing the new concept called *"future cross-functional leadership"*.

The centre of gravity of this paper lies within the expression *"reproductive leadership"* but what it actually considers is the difference between slowly *"straight ahead"* and *"fast forward"*.

WHY WE NEED LEADERSHIP IN THE MILITARY ORGANIZATION

Apart from being a pyramidal system and acknowledging the difference between leading and commanding, leaders are being sought for what they can provide for the group benefit. In this context, there are three key ideas: *survival, purpose* and *achievements*.

Survival, avoiding threats. While encountering problems, as members of a military organization, people will naturally begin to seek guidance, support and leadership from others to minimise threats, which consequently will not diminish their future success and progress; on the contrary, it will help them overcome difficulties and gain confidence.

Purpose. Leaders help people clarify, define, justify and motivate them in relation to why they are doing the work.

Achievement. After motivation, but not before security or survival, leaders are the ones that empower people through their ways towards achievements, rewarding their efforts and helping them becoming successful.

All in all, it is not that these three aspects mentioned above cannot be fulfilled without leaders, but for sure they can be greatly enhanced in the presence of one.

JOHN MAXWELL FIVE LEVELS OF LEADERSHIP[1]

According to John Maxwell's theory, there are five levels of leadership in the military organization:

1. Position/Title. At this level: people follow you because they have to – you are in an official position of authority – and if they do not follow, they could lose their job; upside – at this level, we have the opportunity to define ourselves as leaders and grow; downside – at this level, people who are following you will give their lowest level of energy, engagement, respect, and results. The keyword is rights.
2. Permission. At this level: people follow you because they want to; you have connected with people – there is mutual respect; relationships are the foundation of leadership. The keyword is results.
3. Production. At this level: you are helping bottom line of the company; you are producing results; others follow because of what they see you doing and what results you are producing; you are a model for people; you attract people who want to be like you; you are reproducing others – creating momentum; lots of problem solving by creating momentum. The keyword is relationships.
4. People Development. At this level: you commit yourself to growing/building others as leaders; recruitment is key – the better the people you bring in the *"front door"* the better your organization will be; 80% of success in equipping people to be successful depends on the front door – and who you bring into the company/organization; placement is critical – you must place the right people in the right positions – where they can focus on and hone in on their strengths; successful leaders know how to position other leaders for success – and they are not afraid or intimidated to do so; positioning beats talent alone every time; the focus here is to equip people to succeed. The keyword is reproducing.
5. Pinnacle. At this level: you have done it so well for so long for so many – people follow you – you are the expert; takes a very long time to get there – and very few do it.

LEVEL 4 LEADERS – REPRODUCTIVE LEADERSHIP

In a VUCA[2]-type environment, growing/building others as leaders might be the way to long term success. Underlining the value of level 4 leaders, those that are capable of creating other leaders, must be the key to a problem solving.

[1] John Maxwell, *Five Levels of Leadership*, Editor Center Street, New York, 2013, p. 24.

[2] *VUCA – volatility, uncertainty, complexity, ambiguity*, https://www.wiley.com/en-us/The+Light+and+Fast+Organisation%3A+A+New+Way+of+Dealing+with+Uncertainty-p-9780730328278, retrieved on 10.09.2019.

In what follows we will present four benefits to justify the need for reproductive leadership:

Saving time. Time, an enemy that is always pressing organizations in their pursuit of objectives fulfilment; even worse, technology development has already sped up things around the clock; in order to boost human resource standards and at the same time minimize the gap between great future performance and actual need for improvements we must reproduce leaders; they are the ones that can upgrade the military organization and keep up with a dynamic challenging environment; actually they are saving time.

Efficiency. On a yearly base, military activity has an allocated budget for providing a secure environment, meaning that every single drill or mission is dependent on limited resources; nevertheless, leaders are being able to make the difference between standard performance and efficiency by influencing, motivating and inspiring people to exceed desired outcomes; by adding value in every single key position we can determine an overall multiplying effect.

Organization performance. Seen from a business point of view, leadership is directly related to performance or profit and any leadership will be measured upon this criterion; providing security in a complex environment is actually the military system product or performance; so judging by that, sharing the pieces of this security pie implies having a great amount of leaders able to perform for the military organization.

Fast forward. Neither technological development for the armed forces benefit nor the enemy threats towards security will wait for our slowly response in respect of military proficiency; taking big steps on our way to meet high military standards, level 4 leaders are those who can manage this aspect by acting as a force multiplier within the military organization strength; having them in high numbers will consequently increase leaders presence all over the organization three to four levels down; fast forward stands for a mixture between force multiplier and dynamic movement towards future.

Example. Leaders three levels down. The real strength of an organization is three to four levels from the top. Junior leaders in any organization make an organization great or lead to its eventual downfall. The only way to build a great organization is to build, to maintain, and to continually develop junior leaders three to four levels from the top. These findings are incredibly valuable for a military organization as it seeks to simultaneously improve quality and reduce costs.

Ways to make it happen

Leadership strategy[3]. A leadership strategy is a realistic plan designed to set the level of investment in leadership development so it can meet the standards,

[3] See https://www.ccl.org/articles/leading-effectively-articles/got-a-strong-leadership-strategy/, retrieved on 10.09.2019.

goals and aspirations of the military organization. It specifically refers to how many leaders are needed, what kind of leaders, in what places should they be performing, with what kind of skills, style or acting fashion in order to achieve the desired outcomes.

It also identifies things that need to be changed among the standard system, evaluating criteria or organizational culture, together supporting the leadership that is being created.

Senior leaders need to be able to identify key strategy drivers and their implications for leadership. Implications for leadership strategy – and development of talent and culture – might include: greater interdependence among leadership to create more effective collaboration across war functions or military branches, a need to increase leadership involvement in human resource recruiting, anticipating resources, space, and talent implications of rapidly adapting fighting tactics to ongoing changing threats, a need for cultural change to create a spirit of innovation versus a culture of risk aversion.

A comprehensive leadership strategy translates these implications into specific actions and should take the following five factors into account[4]:

Quantity: How many leaders do we need? What are the current and projected leadership positions on the organization chart? What about informal leadership positions?

Qualities: What characteristics should individual leaders possess? Who needs to be represented or included?

Skills and Behaviours: What skills, competencies, knowledge, and behaviours are needed to implement the military leadership strategy and create the desired culture?

Collective Capabilities: What capabilities do we need so we can act together in groups and across boundaries to implement strategies, solve problems, respond to threats, adapt to change, or support innovation?

Leadership Culture: What are the key attributes of the desired leadership culture? What leadership practices are essential, such as boundary-spanning, employee engagement, or creating opportunities for others to lead?

Centre for military leadership. Be it seen as a self-reliant branch or as a binder between all the military domains, an academic structure that is responsible for teaching leadership in the armed forces is another way to increase the quantity and quality of leadership within military boundaries. Moreover, the existing leadership amongst all ranks will be improved and at the same time kept at the forefront of leadership thinking by courses, evaluations, events and updated publications.

[4] *Ibidem*.

Having this kind of academic tool will help us form, train, promote and reproduce leadership by teaching more about it, talking more about it and furthermore experiencing more of it.

Helping leaders to create leaders. Forming level 4 leaders

Self-awareness. It refers to senior leaders that build their way to the top using a true authentic leadership fashion; they are the key factors, the big wheels that can make the movement faster and smoother; as a real champion says that it is hard to become one but it is even harder to maintain there, so is the senior leadership. Acknowledging the importance of a senior leader role in respect to the followers is the self-awareness that we are talking about; it can be less difficult to develop the leaders below you once you have already made it on your own; undoubtedly, a senior leader has to commit himself to several key drivers like: allocating time and resources, recruiting upon relevant criteria, equipping follower leaders with desirable skills, placing them in the right positions, teaching and coaching, mentoring and acting as a role model for them, truly growing and building them for the benefit of the organizations. Due to little self-awareness, many senior leaders fail the exam of developing the people below them. The impact of this behaviour reflects upon the organizational culture and goals, upon its profit and value. Financing leadership development programmes is necessary but not sufficient coming from a level 4 leader. They must understand that their own leadership effectiveness depends on their willingness to personally and passionately involve in the leadership development of others. Few senior leaders (level 4) are natural leaders of leaders. Fewer are willing, able and motivated to teach, coach and mentor follower leaders. If it is not the self-awareness that makes them conscious of the surviving importance that reproducing leaders is their job, maybe an extrinsic motivation like this article might be the case.

Goals, others and self. These are the three dimensions every single level 4 leader should deal with in his complex pursuit of creating other leaders; setting and prioritizing goals, deepening their understanding of the followers whom they must lead, engage to achieve results; broaden a better knowledge about their own personality while facing the influencing process, self-knowledge.

Involvement. Determining a senior leader to shift from a passive sponsor to the champion of the effort is by making him directly responsible for the leadership development plan; engaging him as initiator of a project is a pragmatic way to change his mindset and behaviour towards full involvement in flourishing follower leaders, while being accountable for the results.

Improving feedback. Even though it is a well-known technique by now, it is actually not efficiently put in practice; level 4 leaders often mistake feedback by criticism or come under the impression that they deliver a quality feedback while there is none or insufficient; the common request of follower leaders to seniors is referring

to feedback, coaching and guidance; on the other hand, delivering efficient feedback can be a difficult thing to do, meaning: creating a dialog, scheduling a programme or a specific frequency which sometimes can be troublesome, proving empathy along while listening, setting common milestones or list of improvements in order to progress as a feedback conclusion.

Counselling, coaching and mentoring. Multiple role playing can be a truly powerful tool in the process of emerging into a genuine leader of leaders. Meaning that different situations require accustomed positions in handling difficulties, ranging from manager, evaluator, boss to a teacher, counsellor, coach, mentor. Should it be clearly asserted, that neither of listed above roles would not replace another nor it could be absent. An effective mixture of target accomplishment, goals achieving with skilful guiding and supporting activity can be the key to this evolving process. The commander carrot and stick alternating with the ear and empathy of the leader might be a winning formula.

Without a doubt, a senior leader's involvement and investment in a development process of followers sends a stalwart persuasive message to them. Let it be known, that level 4 leaders' commitment throughout the reproductive process of leadership, in military organization, is a powerful tool in a challenging performance pursuance.

Key drivers used by level 4 leaders for follower leader development

Territory and clear boundaries. Independence and expansion are representative to emerging leaders; as a senior leader, it is your job to assign a clear area of responsibility, be it in peace times or war, where the follower leader can perform his act of command; at the same time, having more leaders ongoing with the development process implies interfering areas of responsibility, skirmishes also, leaving it to senior leader's competence to deconflict when needed.

Higher progressive objectives. Setting objectives that outclass their previous performance denote a senior leader confidence in a follower potential along with a constructive, challenging path required for leaders to evolve; going above a follower talent and personal effort, designing goals reachable in a collective leading endeavour, a senior leader can motivate in a demanding manner the best of a follower behaviour and qualities; summon a leader to constantly outstand himself is part of a growing process which inevitably reaches desirable outcomes.

Due dates faster than is reasonable. Building a leader requires distinctive means; challenging him to accomplish objectives faster than the average possibilities is a way of stimulating his overall potential; time pressure can be a decisive criterion while testing follower leaders aptitudes; achieving defined objectives in less time or under a countdown heaviness might prove a leader capability to surmount different obstacles and rise above fulfilled goals by using creativity, innovative means, team power, perseverance, resilience and vision.

Stair – stepping their development. A clear leadership development programme should be shared with the participants at the beginning of the process; comprehensive decipherable standards of achievements based on transparent, relevant criteria are to be set and enhance by emerging leaders before commencement; each milestone reached by follower leaders should be embedded with a suitable feedback in respect of their results not before making them aware of their accomplishment within the overall perspective of the entire process ongoing; type of motivation should be noted along the progression.

Skills required for level 4 leaders to lead follower leaders[5]

Strong people skills and interpersonal capability: caring, compassionate, big-hearted; respects people, connects well with others and makes them feel valuable.

Good listener: attentive and present when people are presenting their views.

Team builder: unites, engages, and supports the team's efforts. builds involvement and consensus, supports team members, and advocates for team initiatives.

Leads by example: a good role model *"walks the talk"*.

Visionary: communicates a compelling vision of the future that fosters alignment, knows and sets strategic direction and business plans that allow teams/organizations to thrive.

Personable/approachable: accessible, available, open-door, friendly, likable, easy to work with, and good sense of humour.

Passion and drive: shows passion, enthusiasm, drive, and a strong commitment to the success of the organization and to personal success.

Develops people: shares experience and provides mentoring, coaching, career planning, and development experience to ensure growth and development.

Empowers people: shares leadership and encourages people to take ownership, find their own solutions, make their own decisions, and learn from mistakes; trusts people's ability and their willingness to follow the direction provided.

Positive attitude: optimistic, upbeat; has a can-do attitude.

Methods and tools used by level 4 leaders

Train leaders. It all starts with being intentional about it. Realizing the personal, collective and organizational benefits of helping others to grow might be the key driver in this developing process which ultimately will increase the value of the organization.

Training leaders to evolve via specific development programmes is to be done by those who have been there and done that, senior leaders or as called level 4 leaders. Not apart from diligent, scientific education relevant to this domain carried out by qualified teachers, follower leaders need that kind of touch, influence,

[5] See https://www.leadershipnow.com/leadingblog/2019/02/scaling_leadership.html, retrieved on 10.10.2019.

persuasion, instruction, experience that can definitely boost their potential above standard performance. Pouring into followers, level 4 leaders manage to strengthen the organization from the bottom to the top, raising its worth and image. Coaching correct behaviours and improve individual and group performance over a short or specific period of time. Actually, in the course of time, training, be it formal or informal, has proven a long-life investment, no matter the level of work or type of organization.

Look for potential leaders. First and foremost, this should not be a struggle as looking for a needle in a bottle of hay. People who mirror your best efforts will heighten above the average as determination and willpower are easy to be observed in a competitive environment. These are the people who buy into the vision, who demonstrate initiative, who serve as a reflection of the power of growth. Senior leaders can easily recognize potential leaders if they are willing to do it, by specific markers naturally denoted by them during normal working conditions or challenging environment: great communication skills, asking noteworthy questions, fruitful team working, full commitment to the team success above individual interest, abundance innovative ideas, strong character while sociable and prepared to take charge of the situation no matter the moment. The more this kind of people enter the front door of the organization the greater are the chances of succeeding. They are exactly the kind of people an organization needs to build around.

Mentor developing leaders. Senior leaders should be given effective help, advice and constant guidance over a period of time to follower leaders regarding job evolution. That can be seen as a difficult activity to manage from a timeless perspective, but eventually, it will turn up to be personal task easiness due to a sharing of important organizational responsibilities throughout time. Mentoring emerging leaders signifies making them aware of their talent and potential, supporting them to develop by themselves through guidance and advice over a long period of time. Being a mentor has nothing to do with a high hierarchical position even though might be an advantage, but it focuses on empathy, understanding, helping the follower discover his skills, promote his strong points and upgrade the weak ones. Allocating time for showing a leader the way to progress is of paramount importance to developing followers throughout mentoring. Developing other leaders is a level 4 leader job afterwards. Therefore, it must become a priority.

Move up to new levels of leadership. Undoubtedly, forming follower leaders can turn up, without knowing, into a senior leader blossom. Doing the right things for followers can be an opportunity to move up to the next leadership level. Nevertheless, stepping up means creating more space for emerging leaders coming on the path designed by the senior leader. Setting a leadership reproduction cycle is a great measure of organizational health along with an outstanding desirable

human resource outcome. Moreover, becoming an evolving leader while reaching the highest leadership level betokens the expression *"lead by example"*.

The difference between slowly "straight ahead" and "fast forward" is time

Time to catch up. Military organization needs to move faster if we want to keep up with technological development, with up to date systems of weapons, with challenging security environment, complex overwhelming foreign threats and, last but not least, with NATO partners within the Alliance. Employing level 4 leaders to form follower leaders might be a realistic way to multiply the potential of the entire military organization, by boosting the team performance of follower leaders, therefore the sum of the organization will be greater than the sum of each of its teams. Follower leaders are the ones that can help their teams be prepared by getting different technical courses, making them familiar with new weapon systems, helping them understand the implications of threats against national security and motivating them for daily performance and self-improvement. That is the reason why a military organization should have more of follower leaders raised by senior leaders.

Time for filling the possible hollow of leadership in the military organization. A dynamic environment such as this can be characterized by lots of human resource changes. The flow of personnel between units around the country is a vulnerability when it comes to key positions. Why not having all the time, leaders standing by, ready to replace others that left or fill key positions in less time, thus minimizing the vulnerability of the system.

Time for preparing different generation hand over-take over. The prejudice or experience loss when an elder generation retires or leaves the system is enormous if there is no one to take over from them. Follower leaders can manage properly this kind of issue both in key positions as well as execution or HQ positions. Hand over-take over between generations is a difficult process that entails lots of experience sharing and information passing from one to another. For that there is an obvious need for diligence, foresight, adaptability and innovation, characteristics that belong to senior leaders along with their follower leaders. All in all, the more of level 4 leaders and their followers, the less of military legacy loss while hand over-take over between generations.

Time for saving resources. Leaders capability to boost team performance with the same or less resources needed is already proven scientifically and statistically. It is true that having more of level 4 leaders and thus creating a bigger number of follower leaders is a development investment that is time and resource consuming. But it is also true that, considered as medium- and long-term asset, it will prove resource saving and efficient at the same time.

A suitable example. Let us imagine five company commanders standing in front of an infantry battalion commander while having a discussion about future career plans. Four out of five are well trained in respect of battle tactics, three out of those four are being blessed with potential leadership characteristics like strong personality, a good system of values, foresight, empathy, leading by example, self-givenness and so on and so forth. While only two remaining company commanders possess the necessary motivation to become a battalion commander one day, just one of those two has the circumstance possibility to enlist for specific educational form in order to become a commander. Statistically speaking, we are talking of 1 out of 5 potential candidates for having more of battalion commanders, which obviously is a negative rate after all. Now let us envisage the battalion commander would have been a level 4 leader while standing in front of his subordinates as he had not in the first place. His role now is not only to passively listen to their plans while doing nothing to upgrade their possibilities of becoming more for themselves and for the army benefit, but to play the senior leader role trying to initiate the reproductive leadership process. First and foremost, without any personal effort, only with human resource involvement, he could improve the 5th candidate level of tactical skills through additional training. Secondly, with a few level 4 leadership vision, he might instil some leadership values to the 4th one along with specialized courses in the leadership training institute. Thirdly, using mentoring techniques, he could influence the 3rd one to wish to become a battalion commander foreseeing the benefits of this position. Moreover, he might guide the 4th one for the necessary steps to be taken in order to meet the legal requirement for enlisting at battalion commander courses before being too late. Above all, using coaching and a truly leadership magnetism he could actually boost the chances of the only one existing candidate, the 1st one, in order to be accepted to the battalion commander form of education after passing a complex exam which is already set by default. Nevertheless, a different succeeding rate like 5 out of 5 would have been sketched due to level for leader involvement and reproductive leadership plan. Taking more of a realistic snap shot regarding the rate, 3 out of 5 would still be a positive input for meeting the nowadays needs in terms of leadership positions.

FUTURE LEADERSHIP

The armed forces leadership eventually means leading people throughout other leaders. Creating follower leaders is part of this leadership reproductive cycle along with its benefits. There is still a current controversary discussion upon a matter of autonomy while creating emerging leaders. Future leadership, when talking about forming follower leaders, refers to a quite different perception than the one presented within the article, which happen to show inconsistency and conflictual

ranges of view, but nevertheless, there is a slight difference between a follower leader and a stand-alone leader, both created by level 4 leaders. The difference consists of distinctive behaviours. The first one tends to aim at stepping on the senior leader's path while the second one, more independent, expresses more autonomy, which seems to be a valuable asset in terms of time and resources, from the senior leader's perspective. Instead of cultivating independence in visions and actions, senior leader might prove wrong with the follower leader fashion of growing. This is to debate if suitable to military system from a mission command perspective and a VUCA (volatility, uncertainty, complexity, ambiguity) environment.

CONCLUSIONS

Acknowledging the benefits of reproductive leadership within a military organization means moving fast forward towards modern armed forces development. Level 4 leaders can be used as a force multiplier while meeting the need for leaders in key positions. More of those senior leaders translates into much more of those follower leaders, which ultimately will emerge in possible candidates for replacing level 4 leaders when the time arrives. In other words, level 4 leaders have the ability to reproduce themselves and create a leadership reproductive cycle. Rhetorically speaking, why not amplify the rate of success of company commanders with the battalion commander involvement. Benefits, as mentioned above, can fill the hollow between standard performance and enduring high level of proficiency in a sincere pursuit of future armed forces development.

BIBLIOGRAPHICAL REFERENCE

1. John Maxwell, *Five Levels of Leadership*, Editor Center Street, New York, 2013.

WEBOGRAPHY

1. https://www.ccl.org/articles/leading-effectively-articles/got-a-strong-leadership-strategy
2. https://www.leadershipnow.com/leadingblog/2019/02/scaling_leadership.html
3. https://media.wiley.com/product_data/excerpt/54/11195382/1119538254-26.pdf
4. https://www.i-l-m.com/learning-and-development/management/management-and-leadership-generic/8604-level-4-leadership
5. https://www.managers.org.uk/education-providers/qualification-resource-library/level-4-in-management-and-leadership
6. https://leaderonomics.com/business/maximise-leadership-vuca-world
7. https://www.oxfordleadership.com/leadership-challenges-v-u-c-world/

MYERS BRIGGS TYPE INDICATOR (MBTI) AND MILITARY LEADERS

Marius SUCIU
Master Student "Carol I" National Defence University, Bucharest

Mihai DĂIESCU
Master Student "Carol I" National Defence University, Bucharest

The psychological distribution of military leaders at different levels present interesting patterns. Romanian military leaders have not yet fully appreciated the psychological contributions that staff bring to the resources of the labour force. Human resources, a compilation of the value and importance of the workforce, are a capital investment and should be recognized for the reason of human development and management. This small study conducted with first-year members of the Romanian Staff College found support for extremely dynamic contributions between extraversion and introversion, feeling and intuition, thinking and feeling, judging and perceiving the preferences of future male and female leaders. Military leaders differ in their psychological preferences, and a study like this may predict, on a larger scale, future psychological expectations.

Keywords: personality traits, personality types, leadership, military organisation.

INTRODUCTION

This paper has no intentions on being an in-depth case study regarding MBTI distribution amongst the Romanian Armed Forces and Command and General Staff College. It is rather a more personal point of view in regard to the importance of personality types analysis that make potentially great military leaders. It also tries to illustrate a comparison to old international case studies evolution in this field.

PERSONALITY TYPES

Personality Types Origin

Swiss psychiatrist and philosopher Carl G. Jung developed a theory of personality types in the 1920s. Jung argued that a personality type defines a person in a process, and there are few possibilities for actual achievement or evolution, including leadership. He considers we see reality according to our *"psychological"* type. Jung realizes that many previous theories describe human character in four basic classifications. As for the four elements, for example, astrology classifies the character: water, air, earth and fire. The four basic dimensions of Jung describe how you relate to the world, take information, decide and organize your life. He also divides the four functions into two groups, one for direct experiences and one for the rational organization of the experience. The first group is the feeling of direct experience or intuition, and the second is the planning and organization of experiences. There are two different perspectives, the person inside (introverted) and our relationship with others (extraverted). Jung admits that personality is largely a matter of these functions, and knowing whether a person is extraverted or introverted is the most consistent way to predict people's behaviours.

The Myers-Briggs Type Indicator (MBTI)

During the 1950s, Katherine Briggs and her daughter, Isabel Briggs Myers, broadened Jung's model with the basic improvement of Myers-Briggs (MBTI) indicators. Jung's ideas were refined and put into a language that the average individual could comprehend. Despite the fact that many different scholars have been particularly inspired by identity attributes as a reason for exploring them,

very few of them know about MBTI. Myers-Briggs developed MBTI with the purpose of making Jung's psychological types measurable therefore with a practical importance.

MBTI depends on sixteen distinct psychological types. MBTI considers many equivalent types, not a better or worse combination of capabilities, personality frameworks and conditions, the way we seek and discover fulfilment in everyday life. The clusters used by the Myers-Briggs Type Pointer (MBTI) are based on the foundations of Carl Jung's hypothesis. MBTI is used for certain things, for example, absolute quality management, group building, your and others better understanding, correspondence drawings, relational connections and basic decision-making. Humanity shows a large number of attributes of identity, some studies having an excess of 17,000 qualities. This large group makes it difficult to predict a person's behaviour.

Instead of assessing specific features, traits can be combined and four core groups can be created. Each of us has a percentage of each function, but MBTI determines the extent to which we have developed it and our preferences. This personality indicator allows us to understand the common intersections of our different types. The people we least understand are parts of us that we have not explored well or our contradictions.

The Four Dimensions[1]

a. Relates to the world – their interest mainly derived from the external world of action, objects and people (Extroversion), or an inner world of ideas or concepts (Introversion);
b. Takes in information and ideas – immediate genuine, concrete facts or experience (Sensing) or experiential possibilities, meanings and relationships (iNtuition); (note: since the *"I"* is already used for Introversion, the *"N"* is use for intuition);
c. Makes judgments or decisions – analysing facts objectively and impersonal (Thinking) or weighting values subjectively and personally for the significance of options (Feelings);
d. Controls and organizes people or activities – plan and live in an orderly manner to regulate and control events (Judgment) or robustly and spontaneously to fully understand and adapt to events (Perception).

[1] *Australian Army Leadership Handbook*, 6-3.

The four dimensions define a specific and unique archetype of personality by combining 16 possible types of personality. The results show an extrovert or introvert, sensory or intuitive, thinker or feeler, judge or perceiver. These are 16 permutations of types *(table no. 1)*.

	Sensing	*Sensing*	*Intuitive*	*Intuitive*	
Introvert	ISTJ	ISFJ	INFJ	INTJ	*Judging*
Introvert	ISTP	ISFP	INFP	INTP	*Perceptive*
Extrovert	ESTP	ESFP	ENFP	ENTP	*Perceptive*
Extrovert	ESTJ	ESFJ	ENFJ	ENTJ	*Judging*
	Thinking	*Feeling*	*Feeling*	*Thinking*	

Table no. 1: Meyer-Briggs Sixteen Personality Types

Personality type interpretation determines attitude or functions based on the combination of four letters. The first letter (E or I) is the way we see the world. The second letter (S or N) describes how experience, new information or new ideas are perceived or processed. The third letter describes how we judge, decide or arrange familiar facts or experiences to make them predictable. The last letter tells us how, when confronted with external reality, we usually control and organize people or activities. Analysis of the statistical sample shows that the four categories are not equally distributed among the general population. The distribution is as follows[2] *(table no. 2)*.

Extrovert (75%)	**I**ntrovert (25%)
Sensing (75%)	I**N**tuitive (25%)
Thinking (50%)	**F**eeling (50%)
Judgment (50%)	**P**erceptive (50%)

Table no. 2: Distribution list

These percentages are only approximate, but indicate that *"I"* and *"N"* predilections are in the minority. There is a slight gender shift in the Thinking-Feeling scale, with approximately 60% of all females being *"F"*, and 60% of the males being *"T"*.

[2] From a 1964 study conducted by David Keirsey.

PERSONALITY AND MILITARY LEADERSHIP

"Leadership: The art of getting someone else to do something you want done because he wants to do it".

Dwight D. Eisenhower

The style of a military leader directly affects the personality, temperament and character of the leader. Most of these attributes remain consistent throughout their lives. Part of your knowledge can identify strengths and weaknesses in your leadership style. Leadership requires not only a clear vision of your goals but also the ability to influence your followers to achieve your goals. The style of a leader is called the method presented to achieve his goals.

The style of leadership does not refer both to the way the leader sees it and to its actions, but rather to how others perceive your actions. In the past studies emerged among the leaders, four types of Myers-Briggs personalities: ISTJ, ESTJ, INTJ and ENTJ. Among mid-level officers (captains and majors), two of these four are mostly ISTJ and ESTJ. ISTJ is predominant throughout the United States Military Service and comprises the largest percentage of military leaders. Although only six per cent of the general population is ISTJ, 30 per cent of US military personnel is ISTJ. This considerable five-fold increase is substantial. A high percentage of the three preferences lies in the army, STJ. The combined percentage for US services is 72% **S**ensing, 90% **T**hinking and 80% **J**udging. **E**xtroversion or **I**ntroversion, the first preference varies a little, with about 55% of Introverts and 45% of Extroverts.

	Sensing	Sensing	Intuitive	Intuitive	
Introvert	**ISTJ**	ISFJ	INFJ	**INTJ**	Judging
Introvert	ISTP	ISFP	INFP	INTP	Perceptive
Extrovert	ESTP	ESFP	ENFP	ENTP	Perceptive
Extrovert **ESTJ**		ESFJ	ENFJ	**ENTJ**	Judging
	Thinking	Feeling	Feeling	Thinking	

Table no. 3: Four Corners of Leadership

This means that most of the military leaders are ISTJ and ESTJ. MBTI data from 1999 and 2000 Command and Staff College students, as well as research data from Otto Kroeger, show that this is true. College students accounted for 25% of ISTJ and 19% of ESTJ. Otto Kroeger's results, from 4789 middle-level managers, accounted for 29.6% of ISTJ and 19.9% of ESTJ. This gives credibility to the results of Otto

Kroeger, who does not have a significant difference between civilian leaders and military leaders in medium and high levels of leadership[3]. Both results show that ISTJ, ESTJ, ENTJ and INTJ are the top four types of personalities among middle-level leaders. The micro study conducted within the National Defence University with CGSC students – Land Forces, revealed a slightly different hierarchy.

We used MBTI as an instrument for determining personality types because it is a self-reporting test, easy to administer and with a fast execution. Moreover, having forced answers, the test avoids wrong or false answers.

MBTI test evaluates the strong points of a person in direct correlation with the four dimensions. Also, this test has been extensively researched and validated. The multitude of studies indicated MBTI capability to offer the same or very close data for each iteration for the same person.

In comparison with other tools, MBTI test shows some advantages:

- the simplicity with which the test is implemented and also scored;
- it is based on the Jungian model, an impressively elaborated model;
- the relationship between the test and the possible workplaces suggested by the results.

During this study we used an online personality test form to determine how Romanian CGSC students rank in the MBTI data pool. In the study, ESTJ represents 50% of the total evaluated and ISTJ 12% of it. The surprise discovered at the end of the study was that a fairly high percentage, namely 21%, was ESFJ. The predominant types included in past studies of other armed forces and systems were related to thought and judgment. The highest percentage of leaders fell into one of the four corners when comparing leadership with personality types. In the Romanian study, a fifth type appears to be predominant, namely ESFJ, but it can be considered conclusive only after a future evaluation for the career evolution of these individuals.

The data from Otto Kroeger show that all four of these were common to middle managers, senior managers and executives. Data from Kroeger, made up of more than 13,000 people, show that the more you advance from middle management to the executive, the higher the percentage of the four corners is obvious.

[3] Otto Kroeger, founder of a psychological and management consulting firm in Fairfax, Virginia, has spent 20 years researching large businesses such as AT&T, Xerox, and IBM as well as the United States Department of Defense. He states there is a common myth among corporate, government and military circles that these entities are quite different from one another. His data proved this myth to be false. He proves that *"typologically four-star generals and senior executive service personal are nearly identical to chief executives; majors and government managers closely resemble middle managers in the corporate world"*. Common personality traits among all leaders, military or civilian, mirror one another.

	Sensing	Sensing	Intuitive	Intuitive	
Introvert	**ISTJ 12%**	ISFJ 2.3%	INFJ	**INTJ 4.7%**	Judging
Introvert	ISTP	ISFP	INFP 2.3%	INTP	Perceptive
Extrovert	ESTP	ESFP 2.3%	ENFP	ENTP	Perceptive
Extrovert	**ESTJ 50%**	**ESFJ 21%**	ENFJ	**ENTJ 4.7%**	Judging
	Thinking	Feeling	Feeling	Thinking	

Table no. 4: Romanian Command and Staff College (CGSC) MBTI Results

For example, the four corners represent 70% at middle management level, 73% at the next management level and 85% at executive level. The types of personality at the top level of military and civilian organizations, with 95% thinking and 87% judging, are predominantly TJ. The remaining 5% are Feelers and 13% are Perceivers. Feelers and Perceivers are very poorly represented or non-existent at this level. Either they remained in early positions, enrolled in junior positions, or moved into non-executive roles. The smallest number of personalities in the class of the Command and General Staff class of 2000 is divided into four categories: ISFP, INFP, ESFP and INFJ.

In Romania, the smallest number of personalities in the CGSC class – Land Forces, is divided into three categories: ISFJ, INFP and ESFP[4]. The preference for Feeling is the common preference for each of these types. The relationship between personality traits and personality types of the four corners of leaders can be obtained by analysing the type description. The table below shows the common features. All four types have four common features: integrity/honesty, intelligence/knowledge, initiative and judgment. The four types lack compassion, which Feelers show. Because all four types of thinkers prefer an objective non-personal leadership style, it is logical that compassion is not associated. ENTJ has the most driving characteristics in common with eight; with five, INTJ has the fewest.

[4] See Tabel 4 for data results.

Leadership Traits	Personality Types			
	ISTJ	**ESTJ**	**INTJ**	**ENTJ**
Honesty and Integrity	•	•		•
Intelligence and Knowledge	•	•	•	•
Vision			•	•
Compassion				
Personal Courage	•	•	•	•
Self Confidence				•
Perseverance	•	•		
Enthusiasm		•		•
Initiative	•	•	•	•
Judgment	•	•	•	•
Number in common	**6**	**7**	**5**	**8**

Table no. 5: Analysis of Leadership Traits and Personality Types

CONCLUSIONS

We consider that MBTI has a tremendous importance and validity within an organization, especially a military one, because it can improve climate in the organization. Moreover, understanding yourself and others better, conflicts can be managed easier.

The unique leadership style of a leader is given by the unique blend of features of his personality. Persons with certain personality traits, including integrity and honesty, vision, good judgment, compassion, self-confidence, perseverance, enthusiasm, initiative, intelligence and knowledge, sincerity, humanity, personal courage are more likely to become effective leaders. Regarding these four leadership features, Sun Tzu believed: *"The one who masters them wins, those who are not, are defeated"*[5]. Four types of personalities are usually effective leaders ISTJ, ESTJ, ENTJ and INTJ. They represent about 78% of senior US military officers. All these types of personality include thinking and judging (TJ). These four types, however, account for only 30% of the general population. On the other hand, 95% of the high-ranking military leaders are thinkers, leaving only 5% for Feelers.

Leaders show very little difference in the preference of either being introverted or extroverted. Although most people believe leaders need to have charisma and be heard, data for leaders show that these two preferences are almost equal

[5] Sun Tzu, *The Art of War*, Samuel B. Griffith (ed.), Oxford University Press, New York, 1963, p. 84.

to 50%. Kroeger believes that in order to be successful, organizations will *"need to bring more Feeling and Perceiving types into the upper echelons"*[6].

An absolute military organization will eventually have to become more diverse and creative if the military resources continue to be reduced. Today's armed forces should develop their leadership training, and the promotion system should include a fair approach to Thinkers and Feelers. The system seems to advance those who think about what they feel. The training leadership focuses too much on the knowledge and intelligence of a leader and is not enough to deal with people. I believe that Feelers need to emerge in this area. The solution is a balanced approach to driver training so that a leader displays both goal-oriented attributes. The results of the MBTI Command and Command State College and Kroeger's data show that 80% of medium and high-level senior officers are Introvert-Thinkers (NT) and Sensing-Judgers (SJ). This figure contrasts with only 50% of the same types in the general population. The highest concentration of NT and SJ reaches 85-90% among seniors of all service departments. Data suggest that a military leader career is limited to those who are not represented in the first four types of personality or those that do not reflect an NT or SJ temperament.

At the same time, the study we conducted on a much smaller scale in Romania shows that the future leaders at the Command and General Staff are among the *"four"* corners, bringing an evolution from past studies with the Feelers (ESFJ) being represented as well. Extrapolating, we can say that, after two decades of leadership evolution, Feelers are emerging among leaders. Also, a closer and more extensive look into the personalities of future potential leaders at an early age (during the Military Academy) could help Romanian military human resources to better understand the need of human personnel in certain areas of expertise. The odds are against other types, but they do not need to completely be excluded. Each person has all eight functions, but MBTI only determines the degree to which they are developed and our preferences for them.

There were no differences between military and civilian leaders across the studies conducted in the past using MBTI, therefore, MBTI being used within big civilian companies for work related purposes needs to be taken into consideration by the military structures especially at the beginning of the military career when new, potential leaders do not have enough experience to decide what path to choose. So, some end up in leadership positions or branches with no prospective for leadership and some natural born leaders might be caught in some back office.

[6] Otto Kroeger, Janet M. Thuesen, *Type Talk at Work*, Delacorte Press, New York, 1992, 106 and Appendix B.

BIBLIOGRAPHY

1. ***, *Australian Army Leadership Handbook*. Doctrine Development Command and Staff College, Fort Queenscliff, 2000.
2. Otto Kroeger, Janet M. Thuesen, *Type Talk at Work*, Delacorte Press, New York, 1992.
3. Jane M. Moraski, *Leadership: The Personality Factor*, Virginia, 2001.
4. https://www.armyupress.army.mil(https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160430_art012.pdf)
5. https://www.defence.gov.au/adfwc/Documents/DoctrineLibrary/ADDP00.6-Leadership.pdf.

HOW TO CRAFT THE NEXT GENERATION OF BATTALION COMMANDERS?

Radu PRIOTEASA
Master Student, "Carol I" National Defence University, Bucharest

Marius SUCIU
Master Student, "Carol I" National Defence University, Bucharest

The paper addresses the central role the battalion commanders have in the overall architecture of the military system. The Battalion Commander is close enough to the team so that he can personally interact with every member of the battalion and he also leads a unit large enough to have a major impact on the dynamics of operations (be it in peacetime, crisis or war). The cornerstone of the paper is the attempt to synthesize the essential elements of the ongoing training of these leaders, importance of studying and hard work, delegating punctual tasks to the staff. The essential role of battalion commander in the "growth" of young officers, the importance of tradition, positive motivation and the digitalization of command are as many focal points in completing a "good growth" for the commander as are intriguing topics for any further discussion.

Keywords: commander, battalion, officer, delegate, digitization, motivation.

INTRODUCTION

"2028. In the Middle East, fundamentalist groups have taken control of large parts of the territories of sovereign states. Lieutenant Colonel Daur leads TF 831, a multinational force made up mostly of Romanian elements. TF 831 is responsible for security in the area, maintaining communication practicability main land and also obtaining the support of the local community to combat fundamentalist groups.

A regular patrol on carriers ATEC (Allied Tactical Enhanced Capability), newly acquired by the Romanian Armed Forces, led by Lieutenant Csaba, one platoon leader in Company 2, except that "onboard" is also TF 831 Commander with some staff officers.

With an impressive force under his command (about 1,000 troops), having available increased air support capabilities, intel and support by fire, with the logistical support based solely on national ground, TF 831 mission is the first after the Second World War, when a Romanian Armed Forces unit is solely responsible for an area thousands of kilometres away from the country.

En route to rendezvous with local community leaders, Lieutenant Colonel Daur reviews his notes and browses mentally through the main points of the meeting: greeting ceremony with local leaders, using expressions in Arabic, some references to the historical conflicts in the region, providing support for some local projects seeking the help of local leaders to stabilize the situation.

Self-confidence is the word that characterizes the commander. A safety "contagious" at the level of the headquarters of the unit, and indeed, for all staff. A self-confidence built on passing through all the stages, from platoon to unit commander but with a major milestone represented by the Command Master Degree Lieutenant Colonel Daur got a few years ago.

The two years spent on the "school desks" were, with an intense intellectual and physical effort, a time for "polishing" the next commander: from the lessons in military history to those in leadership, from the map exercises to the numerous seminars held by military personnel, from thorough study of certain combat situations to practical ways to use computers and programmes available to streamline daily tasks, all this amalgam of thoughts crossing his mind at light speed. Since the beginning of the mission he recognized the usefulness of the classes and project planning, the endless MDMP cycles or the saying which became almost a motto for the MC (Command

Master) <better 80% plan completed on time, than 100% too late; realize that more than 100 years of the Military Academy deserve the fame>".

Aside from predominantly SF fragment above it is clear that the battalion commander role in military actions is pivotal. Its role in the architecture of the military system cannot be sufficiently emphasized since it is close enough to the team so he personally knows each member battalion and also leads a structure large enough to have a major impact on the dynamics of operations carried (in peacetime, crisis or war).

But such a person can only be the creation of a rigorous system of military education: from military colleges, continuing with military academies and career courses and, most importantly, what we now call Command Master.

The essential elements of the ongoing training of these leaders are as follows, without us claiming that this list is exhaustive: studying and hard work, delegating punctual tasks to the staff, *"growing"* young officers, maintaining traditions, positive motivation, digitization, command and humour**.**

BATTALION: THE *"BASIC CELL"* OF THE MILITARY SYSTEM

Mărășești, 6 August 1917. Lieutenant Colonel Arthur Vârtejanu, commander of a battalion of the 9th Vanatori Regiment, was ordered to launch a counterattack. Hunters conquered a few tens of meters, being stopped by an artillery barrage. Lieutenant Colonel Arthur Vârtejanu shouted all loud: *"Ahead, guys, follow me!"*.

Despite shooting machine guns and artillery bombardment, our military achieved the objective, but with 16 officers and 500 soldiers died on the battlefield. Among them was Lieutenant Colonel Arthur Vârtejanu. The Romanian Armed Forces reported, after fighting in Mărășești, a number of 27,410 lost soldiers (dead, wounded and missing)[1].

Only one of the hundreds maybe even thousands of examples, many of them unknown, of self-sacrifice and valour, when battalion commanders were decisive on the battlefield.

Online encyclopaedia Wikipedia (in Romanian) provides the following definition for *"battalion"*. Battalion (French Bataillon, Italian Battaglione; in French: Bataille = battle, battle) is a military unit composed of about 300-1300 soldiers made usually of two to seven companies and generally commanded by a lieutenant colonel or colonel. More battalion groups form a regiment or brigade. The Russian Armed Forces battalion has 350-500 people at peace and can go up to 800 people during the war, while a battalion of the armies of NATO consists of 600-900 people.

[1] *Portrete de eroi*, https://once.mapn.ro/pages

Battalion (artillery battalion) is the smallest unit capable of independent military operations. The composition of a battalion in battle resembles squares (spearmen formations arranged in squares with sides of 100 × 100 people, forming a *"forest of spears"*), divided into four smaller squares to reduce losses caused by artillery fire[2].

Battalion and company with their structural elements are the only one in the military system architecture where interaction between members is personal, daily and continuous. These structures, especially the battalion, allows the commander to intervene directly in increased training, cohesion and efficiency of the work performed. Battalion is the structure where one person, in this case the commander, may motivate people in such a manner that the entire staff will modify their behaviour in a radical manner, positive or negative. Battalion is that which, in peacetime, in garrison deployment, can radically change the image of a community on what it means military service. It is through adherence to strict standards of morality, cohesion between members or community involvement. These lines have a single starting point: the battalion commander. But all these potentialities, striving for achievement, require careful planning for each and every step, planning that is based on several qualities previously acquired by the officer who now is in command.

Far from being a closed list, we have chosen out of the many that *"would be nice to have"* seven essential features: study and hard work, delegation of punctual tasks to the staff, *"growing"* young officers, maintaining traditions, positive motivation, digitization command and humour.

STUDY AND WORK HARD TO COMMAND AT BATTALION LEVEL

At a first glance, anecdotally, it seems that between the two is an antagonistic relationship: it may be obvious that if you want to work you will not have time to study and if you want to study while you are in command of the battalion is understood that you will not have time to work.

Personal study increases our speed, creativity and confidence. Without personal study our expertise is limited to our direct experiences. Reading multiplies our experiences in life – as parents, as friends, as spouses and as leaders. Through reading, we can learn from the experiences of a number of people. And, hopefully, reading allows us to learn from others' mistakes, before making the same mistakes ourselves. Old ideas give us new ideas. History really teaches us something. It inspires, motivates and raises us.

[2] Wikipedia, Romanian, retrieved on 25.08.2019.

A personal study plan is an essential component for the development of professional military personnel, especially of those who are in positions of command. As battalion leaders we are faced with a busy schedule every day and finding time to read and think is a recurring challenge. But even as we sign faxes, participate in the training of troops, and find time for sports, we must improve our minds through reading and critical thinking.

Universal Harvard Classics, formerly known as *Dr Eliot's Five-Foot Shelf*, is a collection of 51 volumes of classic works of world literature compiled and edited by Harvard University President Charles W. Eliot and first published in 1909. Eliot affirmed in numerous speeches that elements of a liberal education can be obtained by spending 15 minutes per day reading a collection of books that can fit on a five-meter high shelf (originally, a three-meter rack). Editor PF Collier and Son saw an opportunity and they caused Eliot to do well this statement by selecting a suitable collection of work, and the result was the Harvard Classics[3].

This story could produce in the mind of a decision element, be it even Lieutenant Colonel Daur, a five-foot long shelf collection of books for the battalion commander, collection of which would not miss Sun Tzu, Clausewitz, Plato, Epictetus, Marcus Aurelius, Machiavelli or Westmoreland, and titles belonging to Psychology or Sociology.

In some of NATO partner armed forces there is the so-called *"Professional Reading List"* including a number of books recommended by the head of the General Staff, the head of the Army or Navy, the head Head of the X or Y Department. These lists include titles that vary both in subject (Regional Studies, Strategic Environment, History and Military History, Leadership, Fiction) and scope (from articles, stories, brochures to books). The list is designed to provide subordinates with an idea of the books that influence commanders from different hierarchical levels.

It is clear that for a battalion it is essential, top of the shelf being the leadership books that enhance or improve the efficiency of the work performed. Moreover, the battalion commander is the product of some of the books he reads and whose principles, truncated or integrum, apply to the command position. Study provides the battalion commander with clear thinking and operational flexibility, as well as with coherence, creativity and elegance in speech. The study of not only the doctrine allows the battalion commander to seek and find the best strategies for motivating subordinates, it increases self-esteem and contributes decisively to creating confidence in the act of command. In-depth study removes hopelessly

[3] Wikipedia, https://en.wikipedia.org/wiki/Harvard_Classics, retrieved on 10.10. 2019.

mediocre battalion commander and prepares him or her for the next leadership position.

Hard work at battalion level is, without a doubt, one of the main elements that ensure success as a battalion commander. But philosophy and work ethos are built during years before taking office. Building his or her work philosophy starts from the military academy.

Roman Emperor Marcus Aurelius, the last in a series of *"five good emperors"* of the Roman Empire, known as the king philosopher due to his love for the stoic philosophy, writes in his book *Thoughts to Oneself*: *"I have to go to work – as a human being. What do I have to complain of, if I'm going to do what I was born for – the things I was brought into the world to do? Or is this what I was created for? To huddle under the blankets and stay warm?"*[4].

It requires building a personal ethos of work. This ethos must also be institutionalized as formal as it sounds, and standardized. Recording and tracking tasks, prioritize them and bend to meet the necessary time are essential to the future success of a battalion commander.

To work as a commander is not equivalent to doing all the work. But it is equivalent to unanimously delegate tasks under the argument *"focus on more important things"*. Besides the obvious motivational factor, it is the image of a commander opening a blank Word document and create from scratch a product or device that sits on a battle map.

THE DELEGATION OF PUNCTUAL TASKS TO THE STAFF OR DO NOT DO WHAT OTHERS CAN DO!

"Hard work does not equate with being productive".

Listening to the podcast of Michael Hyatt on the *"Art of Delegation"*[5] we came again to the conclusion that the effective delegation is a fight that military leaders and military personnel battle daily.

Michael Hyatt offers 5 Imperatives of delegation in this podcast, but the real gem of the episode is his description of the 5 levels of authority.

It simplifies the exercise of authority and then clarifies how leaders should delegate.

According to Michael Hyatt, the five imperatives of the delegation are as follows:

Imperative 1: acknowledge that operating non-stop is unsustainable. How many times you saw commanders to begin an exercise or training camp a sleepless

[4] See https://www.businessinsider.com/marcus-aurelius-morning-motivation-2014-8, retrieved on 10.10.2019.
[5] See https://michaelhyatt.com/the-five-levels-of-delegation/, retrieved on 10.10.2019.

marathon? It is as leaders wrongly believe that 1) can sustain that pace, 2) their unit cannot function without them and 3) their physical and mental skills will not fade with exhaustion.

Believe it or not, the same rules apply to daily work in garrison. Leaders who commit, say, working 14-hour days and most weekends will suffer prolonged exhaustion so that their performance deteriorates and causes stress in other areas of life.

Imperative 2: Understand your unique qualities. *"Where to add extra value?".* Maybe you are a remarkable S3 officer, but if you are currently commander, you must focus on being the commander. (On my first day at work, my boss told me: *"I was already chief S3 and I will not do it again. This is your business and I'll let you do"*.)

Imperative 3: Select competent officers to help you.

In a military unit, as well as in the entire Ministry of Defence, it is quite difficult (read: impossible) to *"fire"* someone, as in civilian life. Thus, the unit commander is lacking one of the most powerful coercive instruments available in the market economy: dismissal. Therefore, the future commanders are forced to work with *"client material"* or in Napoleonian terms *"nobody is good at everything but everyone is good at something ... approximate"*.

It is therefore essential to identify the most important abilities that each team member has.

Imperative 4: give those officers the responsibility and authority. We know that military leaders can delegate authority but always retains responsibility for the result. This model allows a leader to be clear about how much authority delegates, which is proportional to the trust he gives to subordinates.

Level 1: Do exactly what I asked you to do.

Level 2: Examine issue and report back.

Level 3: Search the subject, outlined the options and make a recommendation.

Level 4: Take a decision and then tell me what you did.

Level 5: Take any decision you think is best.

Imperative 5: Do only those things which others cannot do. Finally, the delegation fundamental lesson is: Do only what others cannot. If you are in a leadership position, especially if you are a commander, you should not be the one who makes presentations or approves faxes (although it is wise to show that you can still do it occasionally)[6].

[6] *Ibidem*.

"GROWING" YOUNG OFFICERS

Perhaps one of the least publicized aspects of the responsibility for future battalion commander is mentoring young officers of the battalion. Currently, the situation can be briefly classified as follows: *"before the Command Master no one teaches you; after you get to be the commander you have no time"*.

In the absence of a regulatory framework to conduct this activity, apart from technical aspects (the time of the year, documents drawn up, points awarded etc.), the future commander has no support.

In one of the studies that led to the introduction of mentoring young officers in the US military it is stated that *"mentoring is needed ... when the battalion commanders invest time in guiding young officers, young officers understand the organizational structure, environmental dynamics and personalities that contribute to better decision-making capacity"*[7].

Mentoring has resulted in numerous benefits for the military, such as producing future leaders who are more confident, better educated and more satisfied with their work and career advancement. In addition, young officers are more receptive to accepting the Armed Forces objectives, which gives a greater sense of belonging and acceptance in the organization.

The lack of an adequate institutional framework should not discourage future commanders of battalions to create a recipe of own mentoring young officers according to their vision. The task will not fall into the ridiculous if prospective mentors are nominated among the best of the unit officers: commander, deputy commander, chief of staff, chief S3 and other officers elected *"with care"*.

Increased attention to grow young officers is one of the processes whose fruits will be seen over 5, 10 or 15 years and some of the causes of the current deficiencies in the military system can be identified in (lack of) mentoring 5, 10 or 15 years ago.

MAINTAINING TRADITIONS

Article 157 of the *Rules of Procedure* [8](only result observable from a Google search after *"military traditions"*) states that: (1) Meeting military traditions of the unit is set up in brigades, regiments and battalions approved by the chief of staff of the category of military forces or Commanding weapon and for cultivation fighting traditions of the army, weapons and unity and development institution, soldierly

[7] See https://www.researchgate.net/publication/235023199_Mentoring_Junior_Leaders_Leadership_Tools_For_Our_21st_Century_Army, retrieved on 10.09.2019.

[8] See https://lege5.ro/Gratuit/gmztkojsgy/art-157-activitati-organizate-la-clubul-unitatii-sala-de-traditii-militare-filiale-ale-muzeului-militar-national-regulament?dp=gyzteojrge3dq, retrieved on 10.09.2019.

respect to specific values and worship for heroes. (2) In the hall are exposed traditions, respecting the principles of museological objects, uniforms, weapons, equipment, decorations, signs, documents, photographs and other materials relating to the unit past, from the beginning until the current period. Theme exhibition highlights organizational transformations, participation in military campaigns, heroes and great personalities of the unit, procurement and procurement development, the main missions fulfilled over the years, including the economic and social ones. (3) The military educational institutions and the headquarters of large units, depending on the property, technical and material, financial resources and trained personnel with the approval of the Minister of Defence may establish branches of the National Military Museum. They are part of the military museum and are open for both the military and the public.

Also, the same search presents some activities of the Military Traditions Section and also the sequence of events in which the *"Military Traditions Association"* (in fact, a squad that has military uniforms from the First and the Second World Wars) took part.

In essence, we believe that the military traditions are those elements of worship (heroes, items, days, events etc.) for a military unit, which pour upon the members of that unit. Of course, the traditional National Day military parade is a military tradition but what can a young future battalion commander do at a more tactical level?

Surely anchoring the regulatory provisions and the creation or renovation of tradition is a beginning for future battalion commanders. But further, what is the plan?

The plan is reviving and building traditions related to the past of this unit. Identifying a personality, a heroic battle, a symbol (flag, emblem, act of courage etc.) to be celebrated regularly or a unit ball make the members of that structure to build membership in some common history. Beyond the symbolic nature of this gesture, such a tradition could have the following positive results:

- building a membership of a common symbol;
- joint activities which would involve the majority of the members of the unit;
- a test for battalion commander;
- another test for the entire unit to find cohesion structure.

Obviously for the future battalion commander the *"traditions test"* is another tool at hand to build a team in every sense of the word. But this requires a few ideas, positivity and consistency in pursuing these ideas.

POSITIVE MOTIVATION

Positive motivation is produced by stimulation awards: praise, encouragement, promises of material rewards and moral activation of positive feelings etc. The beneficial effect on those who receive them is increasing their efficiency in study and work. This type of motivation acts as *"sugar"* in Pavlovian conditioned reflex learning.

In an era of global communication, facilitated by the movement of information with the internet speed, mediated by social networks, it is clear that for most of the force of the military system, positive motivation exercised by the chain of command is the norm. Psychological incentives as well as those having a material nature have an overwhelming influence on the staff performance. And when these tools are used in accordance with a plan established before and according to scientific principles, it is likely to succeed.

Moreover, although the future battalion commander retains the line of duty and the coercion tool, it is desirable for the future commander to operate using positive motivation levers in most of situations. Positive incentives bring long-term benefits, for the students of military academies included, both by stimulating non-verbal behaviours (smile, approving non-verbal face-to-face discussions, calm tone) and by using words and positive expressions. These exercises are necessary to be continued, refined and enhanced during the Command Master, being the last long training before assuming command by future commanders of battalions.

Beyond the near-universal acceptance that *"positive rewards produce more beneficial and long-lasting results than the negative"*, institutionalization and a scientific approach in all forms of education are required. Without identifying positive motivation as a panacea for the whole range of issues that may exist at a military unit level, in this case battalion, it must nevertheless be admitted the superiority of this approach to the negative one based on punishment.

The future battalion or Task Force commander, be it even Lieutenant Colonel Daur, should be taught in the training forms earlier that *"bringing more sweetness"* and a positive approach to the members of the staff and more, to the entire unit, is more productive and efficient in the long term.

COMMAND DIGITIZATION

In the social media era, likes, sites, sharing, bits and bytes, it is anachronistic for future commanders of battalions to give up their advantage of using technologies.

The future battalion commander is not afraid of the computer and all that it brings with it. From a master of PPT, Microsoft Word and Excel to a certain

familiarity (I heard of ...) with NATO software, the commander conquers the digital terrain.

From *"the simple"* Outlook, whose usages in daily work are countless, to systems of command and control that are available to each compartment (from S1 to S6) to enhance efficiency, modernization and adjustment work, they are almost endless.

Team members (of the unit) can become more efficient, more organized and more proactive using these tools. To streamline work within the structure the future battalion commander will lead, it would be to make use of these tools. Specialized seminars, within the Command Master programme, will provide some of the newest trends in specific SOF or C2 applications. But beyond that, he or she will master several instruments within Outlook, which simply make life easier: disable Outlook if you have a task to do. There was once a *"multitasking"* God. It was a false god. The truth is that if the tasks are complex, you have to focus on them. An officer working tirelessly cannot provide quality analysis; understand the difference between the To: and Cc: boxes Address To: and Cc: If I send an e-mail and are Cc box: I will read after you delete it. If you are in the To box: I will seek what to do.

Sometimes you have to send an e-mail with the same information to several persons. Sometimes you cannot contact that person. Usually, if you need an answer in less than 24 hours, call. In fact, it may be quicker to call someone to explain the context of the question or problem, then to send an e-mail. Not only is it faster, but the person on the other end will thank you. He or she might be able to respond verbally to questions.

HUMOUR

Used properly, good humour and mental and physical wellness provide huge benefits for us as leaders and for those structures that we lead. A joke or irony has both cognitive and emotional impact.

A study by the Mayo Clinic states that there are many benefits of laughter in the short and long term. It can soothe away tension, can stimulate organs by increasing endorphins and natural reaction to stress, can activate the body. Long-term benefits include increased immune system, improved mood and life satisfaction. Prospective battalion commanders must know the right time to use humour.

Marshal William Slim is one of the most revered leaders of British and Australian armies. As commander in China-Burma-India theatre during the Second World War, Slim believed that keeping the sense of humour is essential to survive the harsh realities of combat. During a tough fight that demoralized people, he saw the need to improve the mood among the forces.

"Well, gentlemen, it could be worse". "How?" "Well it could rain", and two hours later it started to rain[9].

Humour is not only beneficial to the atmosphere of the battalion but also desirable. And, the battalion commander is supposed to build a work-friendly climate step by step.

Humour is innate to some of us. To others, the majority, it can be learned. There are countless resources both in the classic format and especially on the internet that can teach you how to make if not extraordinary jokes at least some good ones.

In the case of most of us, great commanders are made, not born. And this does mean transformation, work, study and ... from the beginning again. Without an internalization, a solid scientific basis and a consistent inclination to become better as military professionals, we, the future battalion commanders, will self-indulge in overwhelming mediocrity.

BIBLIOGRAPHY

1. ***, *Portrete de eroi*, https://once.mapn.ro/pages
2. Marcus Aurelius, *Gânduri către sine însuși*, Editura Humanitas, București, 2013.
3. Michael Hyatt Podcast, https://podcasts.apple.com/us/podcast/042-fine-art-delegation-podcast/id502414581?i=163417035&mt=2
4. Wikipedia, https://en.wikipedia.org/wiki/Harvard_Classics
5. https://fromthegreennotebook.com/2014/11/20/levity-in-leadership/.

[9] See https://fromthegreennotebook.com/, retrieved on 10.19. 2019.

PAGES FROM THE ROMANIAN MILITARY THINKING. THE POLITICAL-STRATEGIC VISION ON (NORTHERN) DOBROGEA: 1878-1913

George UNGUREANU, PhD

Romanian National Military Archives – Military Archive Centre, Piteşti

Starting from the complexity of the defence and national security field, this article, based on Romanian, Western, Bulgarian and Turkish historiographical contributions, supplemented with archival military documents, deals with the problem of defence of the right bank Danube territory obtained after the Berlin Congress (1878), until the incorporation of Southern Dobrogea (Quadrilateral) in 1913. This article briefly shows the initial Romanian views on the inclusion of Dobrogea, then the measures enforced by the authorities at two levels, namely the political-diplomatic and military one, and the ethnopolitical one respectively, including economic, social and cultural aspects. The conclusion is that the military measures taken led to limited achievements, mainly due to some objective reasons, but this situation was counterbalanced by suitable political-diplomatic combinations and options and especially by the remarkable result of the work aiming to enhance, modernise and colonise the territory. A decisive stage in this respect was that of 1890-1895.

Keywords: borders, internal vulnerabilities, external threats, projects, actions, evolutions.

For specialists in the field today, it is almost a truism to say that the problem of the national security and defence sciences involves only political, diplomatic, military and intelligence (or counterintelligence) aspects. It has a much wider and more complex scope. The various realities and the economic, social, cultural, collective-mental and axiological developments represent potential vulnerabilities or strengths of the national defence and security system[1].

Regarding the historical Dobrogea, its generally accepted geographical limits are represented by the branched course of the Lower Danube (with Balta Ialomiţa and the Big Island of Brăila) to the west, the Black Sea to the east, the Lom-Provadija river line to the south and, respectively, the Danube Delta to the north[2]. Some authors, however, exclude the southern forest area (Deliorman) from the whole of the Dobrogea lands[3] while a local toponymic tradition identifies the province, exclusively with the central steppe area, excluding both the Southern Deliorman and the so-called *"Northern Deliorman"* (the hills of Tulcea)[4].

After the Russian-Romanian-Turkish war of 1877-1878, the territory of historical Dobrogea inhabited by a very diverse ethnolinguistic and religious population was divided between independent Romania (the northern, including the Danube Delta, and central areas) and autonomous Bulgaria (the southern part). After this date, in the Romanian media, the word *"Dobrogea"* began to designate, in particular, that trans-Danube territory that became part of Romania in 1878. The situation has been perpetuating so far, except for the period 1913-1940, when Southern Dobrogea (Quadrilateral) was part of the Romanian state. In contrast, in the Bulgarian media, the term *"Dobrudža"* is used with its maximum historical meaning, sometimes specifying the distinction between Northern Dobrogea (belonging to Romania) and Southern Dobrogea (belonging to Bulgaria).

We intend, in this study, to draw/shape the main coordinates of the Romanian political-strategic conception of defence and integration of the territory on the right side of the Danube added after the Berlin Congress (1878) until 1913, when,

[1] See, for instance, the study of George Ene, *Eminescu, securitatea şi siguranţa naţională a României*, Editura Eikon, Cluj-Napoca, 2014, *passim*.

[2] Joseph V. Poppov, *La Dobroudja et les relations bulgaro-roumaines*, Liège, 1935, p. 13; Constantin Brătescu, *Morfologia Cadrilaterului*, Cernăuţi, 1938, pp. 1-2.

[3] A. Ichirkoff, *Géographié physique de la Dobroudja*, in *La Dobroudjja* edité par l'Union de savants, artists et ecrivains bulgares, Sofia, 1918, pp. 2-3.

[4] Lt.col. Ioan Munteanu, *Cadrilaterul, istoria unei controverse* (*1878-1919*), in *"Anuarul Institutului pentru Studii Politice de Apărare şi Istorie Militară",* Bucureşti, 1997, p. 181.

through the Bucharest Treaty, Romania got the Southern Dobrogea (Quadrilateral) from Bulgaria. More specifically, we will show the initial Romanian opinions (1878) on the possibility of, then on the actual inclusion of Dobrogea, as well as, in particular, the measures taken by the Romanian state and its institutions regarding this province, both at the political-military and the ethnopolitical level.

In principle, an increase in the surface area and population of a state represents a potential progress factor, but for a complete evaluation other factors (geographical position, natural resources, communication means, level of development, possibilities and system of integration of the obtained territory) must be taken into account[5]. In the light of such a conception, but also for other reasons of principle and political opportunity, at the beginning of 1878, the Romanian decision-makers (King Carol I, Ion C. Brătianu Government, the Assembly of Deputies and the Senate) categorically rejected the idea of the territorial exchange proposed by Russia (South Basarabia for Dobrogea and Ludogorje, up to the Ruscink-Varna line), without completely excluding the possibility of obtaining territories beyond the Danube[6].

On the general background of rejecting the Russian claims, there were also voices of some Romanian politicians and publicists, who saw Dobrogea as *"a poisoned fruit"* offered by the Russian Empire to small Romania, or even as a Bulgarian territory[7]. In the memo addressed by the Romanian government to the European cabinets, in February 1878, it was requested that South Basarabia remained part of Romania and that the Danube Delta was given to Romania, in order to provide more economic development possibilities for the Romanian state and to ensure freedom of navigation on the Danube for European states. The idea of adding Dobrogea to Romania was rejected with geostrategic and geoeconomic arguments (isolation of this province from the Romanian territories on the left of the Danube and the consequences of this fact for the future development of the country)[8].

Facing the categoric Romanian refusal, considered offensive, Czarist Russia decided to cut the territory of the compensatory offer for southern Basarabia. Thus, through the Treaty of San Stefano (19 February/3 March 1878), the northern border of Bulgaria was settled in the vicinity of the strategic line Cernavodă-Constanţa,

[5] Constantin Iordan, *România şi relaţiile internaţionale în sud-estul european (1919-1924). Probleme ale păcii, securităţii şi cooperării*, Editura ALL, Bucureşti, 1999, p. 12.

[6] Nichita Adăniloaie, *România independentă* in *Istoria românilor* (academic treatise), vol. VII, T1; *Constituirea României moderne (1821-1878)* 2nd edition revised and added, coord. : acad. Dan Berindei, Editura Enciclopedică, Bucureşti, 2015, pp. 749-750.

[7] See Antonina Kuzmanova, *Le caractére bulgare de la Dobrodja vu par les Roumaines. Propagande et mise en comideration des réalités (1878-1944)*, in *"Etudes balkaniques"*, 29, nr. 31, 1993, pp. 3-5.

[8] Sorin Liviu Damean, *România şi Congresul de Pace de la Berlin (1878)*, Editura Mica Valahie, Bucureşti, 2011, pp. 55-56.

passing through Rasova[9], and Russia reserved the right to maintain the connection with its troops from Bulgaria (also) through the Romanian territory[10]. However, in an attempt to protect the susceptibility of Western powers, Russian Chancellor A.M. Gorceakov said: *"The Romanian Dobrogea will separate the Russian Empire from the Bulgarian state"*[11]. However, the partition invoked by Gorceakov was a thin and rather permeable one. In addition, the offer from San Stefano gave Romania a narrow part of the coastline, necessary for the development of a large port. The initial offer, the one from January 1878, was viewed by Romania with circumspection because of the difficulty of integrating a large territory (over 25,000 km2), with a majority Muslim-Turkish-Tartar population and a significant share of Bulgarian ethnicities. On 27 March/8 April 1878, about 200 representatives of Muslims, Greeks, Armenians and Jews from Dobrogea, led by the Turkish mufti and the Greek archimandrite, signed a document requesting that Romania should receive the entire Dobrogea and the Varna port city, with its hinterland[12]. An advantageous solution for the Romanian state, in 1878, could have been the establishment of the border on the Rusciuk-Varna line, but only under the conditions of a population exchange involving the Romanian ethnic groups from the Vidin area and the Dobrogea Bulgarians[13].

Russian diplomacy failed to temper the apprehensions of the Great Western Powers, so the provisions of the Treaty of San Stefano were substantially revised, following the Berlin Congress. By the Treaty concluded in the German capital, the re-annexation of Southern Basarabia to Russia (Art. 45) was approved, and Romania obtained the Serpent Island, the Danube Delta and the northern and central parts of Dobrogea, up to a line between Silistra and Mangalia, whose delimitation *"on the ground"* was the task of an international commission (Art. 46)[14].

British Balkanologist William Miller estimated half a century after the events that the land border established in Berlin had been "*unsatisfactory for both sides"*, because "*it gave strong fortresses to Bulgaria, with which it dominated Dobrogea, and to Romania it gave its actual possession"*[15].

[9] Stajko Trifonov, *Dobrudžanskijat văpros (1878-1944)*, in *Novi očerci po bălgarskata istorija (1878-1948)*, coord.: Marija Radeva n.p., Sofia, n.y., p. 191.

[10] *Istoria politicii externe românești în date* (will be quoted as *I.P.E.R.D*), coord.: Ion Calafeteanu, Editura Enciclopedică, București, 2003, p. 180.

[11] Constantin Iordan, *Dobrogea (1878-1940) în istoriografia bulgară post-comunistă*, Editura Academiei Române, Bucureşti, 2013, p. 24.

[12] Alexandru P. Arbore, *Noi informaţii asupra Dobrogei*, in „Analele Dobrogei", XI, Cernăuţi, 1930, pp. 88-89.

[13] George Ungureanu, *Problema Cadrilaterului în contextul relaţiilor româno-bulgare (1919-1940)*, Editura Istros Publishing House, Brăila, 2009, p. 39.

[14] *I.P.E.R.D*..., p. 181.

[15] William Miller, *The Ottoman Empire and its Succesors (1801-1927)*, Cambridge, 1927, p. 400.

The head of the Romanian government, Ion C. Brătianu, showed that his country was an outpost of Western civilisation in the proximity of Russian despotism and post-Ottoman barbarism: *"When we were given Dobrogea, Europe gave it to us out of a European interest, because they believed we were not only a brave nation, but also one of the most civilising nations in the East"*[16]. Discovering the geopolitical and geostrategic reasons for the decision of the European Areopagus, Captain Marin Ionescu Dobrogianu (1866-1938), wrote, a quarter of a century after the events: *"If Russia occupies Dobrogea, the European Danube Commission becomes a cosmopolitan island, in the middle of a Russian sea"*[17].

The first Romanian military detachments entered the Trans-Danube province on 14 November 1878, when a proclamation of Carol I was issued to the locals, and the Romanian administration was installed starting 23 November, the last Russian troops leaving the area in April 1879[18]. The Serpent Island actually came under Romanian military control on 12 April 1879[19]. The *"on the ground"* delimitation of the Romanian-Bulgarian border was made with difficulty and tension, the incident from Arab Tabia (today Ostrov, Constanţa county), from January 1879, between the Romanian and Russian military, being very famous; finally, the Romanians were very affected by the fact that Silistra and the fortified points Medgidié-Tabia and Ordo-Tabia, in its proximity, remained in Bulgaria[20].

The territory of Dobrogea obtained by Romania in 1878, amounting to about 15,600 km2, was strategically dominated by the Cernavodă-Constanţa and Valea Carasu lines, having, according to the 1880 census, a population of 147,247 inhabitants, of which 44,354 (16,448 + 27,906) were Turks-Tartars (11.2% + 19.0% = 30.2%), 40,449 Romanians (27.5%), 29,440 Bulgarians (19.9%), 9,683 Lipovans and 8,348 Russians (6.5 % + 5.6% = 12.1%), 6.481 Greeks (4.5%), 3,147 Jews (2.1%), 3,030 Germans (2.0%) etc[21]. Except for Bulgarian historians, foreign (western) historiography considers that the territory obtained by Romania in 1878 was an exceptional ethnic mosaic, with a relative majority of Turks-Tartars, followed by Romanians and Bulgarians[22]. However, the various ethnicities were spread far and wide: Bulgarians were more numerous in Tulcea county (N), where the majority

[16] Apud Valentin Ciorbea (coord.), *Dobrogea (1878-2008). Orizonturi deschise prin mandat european*, Editura EX PONTO, Constanţa. 2008, p. 17.
[17] Marin Ionescu Dobrogianu, *Dobrogea în pragul veacului al XX-lea. Geografia matematică, fizică, politică, economică şi militară*, Atelierele grafice Socec, Bucureşti, 1904, p. 916.
[18] Adrian Rădulescu, Ion Bitoleanu, *Istoria Dobrogei,* second edition, Editura EX PONTO, Constanţa, 1998, pp. 349-351.
[19] M. Ionescu Dobrogianu, *op. cit.*, p. 305.
[20] Daniela Busă, *Modificări politice şi teritoriale în sud estul Europei (1878-1914)*, Editura Paideia, Bucureşti, 2003, pp. 48-57.
[21] Robert Stănciugel, Liliana Monica Bălaşa, *Dobrogea între secolele VII-XIX. Evoluţia istorică,* Editura D.C. Promotions, Bucureşti, 2005, p. 203.
[22] G. Ungureanu, *op. cit.*, p. 38.

of Russians and Lipovans lived and Turks-Tartars were predominant in Constanţa county (57%), and the Romanian ethnics lived mainly in the proximity of the Danube and its ponds, arms and mouths[23].

It is not irrelevant that the population density in the area was low, under 10 inhabitants per km2, while on the rest of the Romanian territory it had reached the level of 34 inhabitants per km2 two decades before[24], which was a favourable premise for the future work of colonisation.

From November 1878 until March 1880, Dobrogea was under the regulatory regime. On 9 March 1880, the *Law on the organisation of Dobrogea* was promulgated, drafted by Mihail Kogălniceanu and magistrate Remus Opreanu, the Prefect of Constanţa[25]. According to this act, Dobrogea did not yet have representation in the Parliament of București (it was to acquire it in 1909), the communal councils elected the county councils of Constanţa and Tulcea, and they submitted to the ruler (since 1881, the king), an annual report also including their desires[26].

For the young Romanian unitary state, immediately after the War of Independence, Russia had imposed itself as the greatest danger to its sovereignty and territorial integrity, which resulted in the secret accession to the Triple Alliance (18/30 October 1883), and subsequently, the creation of the fortified line Focşani-Nămoloasa-Galaţi, with the direct participation of German Major M. Schumann (1888-1893). As for Dobrogea, more direct Romanian fears were related to small Bulgaria, dissatisfied with the territorial clauses of the Berlin Treaty. When voting the Turnovo Constitution (1879), delegates of the Bulgarians from Northern Dobrogea also took part, and *"the statement that Dobrogea is a Bulgarian territory inhabited first of all by the Bulgarians, taken away from Bulgaria and given to Romania, in exchange of Basarabia, is invariably included in the school textbooks and Bulgarian reference papers after 1878"*[27].

The Romanian-Bulgarian territorial rivalry evolved within the wider framework of the political-diplomatic and military relations at the European level. While Romania roughly gravitated on the orbit of the Central Powers, Bulgaria alternated between Russophile and Russophobe cabinets. As a result, the Romanian-Bulgarian relations reached their cordiality peak under the rule of Russophobe liberal leader Stefan Stambulov (1887-1894), known

[23] R. Stănciugel, L.M. Bălaşa, *op. cit.,* p. 203.
[24] Keith Hitchins, *Românii (1866-1947),* third edition, translation by George G. Potra and Delia Răzdolescu, Editura Humanitas, Bucureşti, 2004, p. 163.
[25] A. Rădulescu, I. Bitoleanu, *op. cit.*, p. 353.
[26] *Ibid*, p. 354.
[27] Blagovest Njagulov, *Les images de l'autre chez les Bulgares et les Romaines (1878-1944)*, in *"Etudes balkaniques"*, 31, nr. 2/1995, p. 5.

for these words: *"If Romanian Dobrogea had not existed, it should have been invented, to separate Bulgaria from Russia"*[28]. At the opposite pole, we can mention the aggressive Bulgarian actions at the border, in August 1885, encouraged by Russia[29], as well as the Russian-Bulgarian secret conventions of 1902 and 1909, which confirmed Russia's promise to support the Bulgarian territorial ambitions in Northern Dobrogea, if Romania were to fight against the Great Power from the East, in a general conflict, a known commitment in București[30]. Moreover, according to military historians Momčil Ionov and Stančo Stančev, Bulgarian military experts considered at the beginning of the 20th century that Dobrogea would be the main battle theatre, in case of a Romanian-Bulgarian war[31].

We will further address the political-diplomatic and military actions taken by Romania to defend the threats coming from Dobrogea, including the idea of annexing the Southern Dobrogea to the Romanian state.

The main politico-diplomatic instrument for the defence of pre-war Romania, including Dobrogea, was the secret alliance with Germany, Austria-Hungary and Italy, signed on 18/30 October 1883 and renewed successively in 1888, 1892, 1902 and 1913[32]. However, the act concerned only Russia and the eventuality of an unprovoked aggression on its part. Romania's attempts to include a clause regarding Bulgarian were not successful[33]. However, the possibility of a Russian-Bulgarian conjugated act was at least theoretically counteracted. Mentioning such an eventuality, M. Ionescu Dobrogianu wrote, in 1904: *"We would be overwhelmed by forces and circumstances. But in this case, the problem is complicated: we have allied armies on our side..."*[34].

In October 1884, the meeting in Rusciuk, between King Carol I and Prince Alexander of Battenberg, determined the military situation at the Romanian-Bulgarian border for the next several months[35]. We cannot say the same about the high-level official visits of 1897, 1902 and 1909, which were less fruitful and could not remove the general atmosphere of mutual suspicion[36].

[28] *Apud* Hristofor Hesapciev, *Amintirile unui fost diplomat bulgar în România (1905-1910),* translated by Daniel Cain, Editura Fundația PRO, București, 2003, p. 42.
[29] Daniela Buşă, *op. cit.*, pp. 56-60.
[30] Gheorghe Zbuchea, *România şi războaiele balcanice (1912-1913). Pagini de istorie sud-est europeană"*, Editura Albatros, 1999, p. 70.
[31] *Apud* Gavriil Preda, *Relaţii militare româno-bulgare la sfârşitul secolului al XIX-lea şi începutul secolului al XX-lea*, in *Români şi bulgari. Provocările unei vecinătăţi,* coord.: Fl. Anghel, Mariana Cojoc, Magdalena Tiţă, Editura Cartea Universitară, Bucureşti, 2007, p. 122.
[32] *I.P.E.R.D.*, pp. 191, 208.
[33] Petre Otu, *Bulgaria în planurile de campanie ale armatei române în anii 1912-1916*, in *Români şi bulgari…*, *op. cit.,* pp. 151-152.
[34] M. Ionescu Dobrojeanu, *op. cit.*, p. 924.
[35] D. Buşă, *op. cit.*, p. 58.
[36] G. Ungureanu, *op. cit.*, pp. 201-206.

It is also worth mentioning that the interests of 13 states were represented in the Romanian Dobrogea, at consular, vice-consular or commercial agency level: Great Britain, Austro-Hungary, Belgium, Denmark, France, Germany, Greece, Italy, The Netherlands, Russia, Spain, Sweden and the Ottoman Empire[37].

Due to the varied ethnic composition of the Dobrogea population, a potential danger for the Romanian administration was represented by the local irredentist organisations and actions, in this case, the Bulgarian ones. Some irredentist leaders, once discovered by the authorities, left (voluntarily or forced) the province, among them the father of the poet Panait Cerna (1881-1913); the remaining ones turned mainly to the political left (the Socialists, the Peasant Party), anticipating a trend that would manifest itself fully in the inter-war Quadrilateral. The local Romanian-language press repeatedly drew attention to the prosperous material situation of the Bulgarian communities, which allowed them to finance subversive activities, camouflaged in cultural activities[38]. In principle, the minority schools were free, only the teaching of the Romanian language being compulsory[39]. The suspicions that were hovering over the ethnic Bulgarians from Tulcea county caused prefect Ioan Neniţescu, known especially as a Romanian nationalist poet, to resort to a series of punitive and restrictive measures, in 1898: the abolition of Bulgarian *"communities"*, schools and cultural houses, expulsion of teachers from Bulgaria and limited study of the mother tongue to one hour per week[40].

Much more loyal to the Romanian state, even if it was a more passive loyalty, were the Dobrogea Muslims, a fact understood and appreciated by the rulers; In 1880, the great vizier Said Pasa expressed to the plenipotentiary minister in Constantinople, Dimitrie Brătianu, the gratitude for the attitude of the authorities and the Romanian population towards the Muslims in Dobrogea[41].

At the military level, we note, first of all, the placement of the 5th Army Corps in the area, namely the establishment of the Romanian military navy (1883), with 1898 as a reference year, when the Danube Division and the Sea Division were created. Around the First World War, the Danube Division included three groups, namely: the Danube Squadron (4 monitors and 8 stars), the Galați-Tulcea-Sulina area Defence Group with 4 checkpoints, 3 torpedoes – *"Năluca"* type, 3 boats –*"Rândunica"*, *"Ştefan cel Mare"*, *"Alexandru cel Bun"* type, as well as artillery battery and, respectively, the Cernavodă-Feteşti defence group, 4 canons and 4 *"Vedea"* type

[37] A. Rădulescu, I. Bitoleanu, *op. cit.,* p. 372.
[38] Mădălina Lasca, *Imaginea comunităţilor bulgare din Dobrogea în presa de limbă română de la sfârşitul secolului XIX"* in *Români şi bulgari…*, pp. 89-104.
[39] A. Rădulescu, I. Bitoleanu, *op. cit.*, p. 355.
[40] Ioan N. Roman, *Iredenta bulgară în Dobrogea*, in *"Analele Dobrogei"*, XVI, Cernăuţi, 1935, pp. 5-6.
[41] A. Rădulescu, I. Bitoleanu, *op. cit.,* p. 360.

boats. The Sea Division included the cruiser *"Elisabeta"*, the *"Mircea"* brig and the navy schools. The total crew number was 2,562, of which 147 were officers and assimilated, 98 masters and civil craftsmen. However, a whole host of shortcomings overshadowed these achievements. The cruiser *"Elisabeta"*, considered, at the time of its launch (1888), the most powerful warship in the Black Sea, was used up before the outbreak of *"the Great War"*, the light torpedoes were not very stable during bad weather, and the *"Mircea"* brig had a reduced combat ability[42].

If the Bulgarian fleet was weak, the Russian fleet represented a very dangerous potential opponent, an attack of which could, in the opinion of Marin Ionescu Dobrogianu, most likely target the Constanţa-Cernavodă line, and not Mangalia, defended by the homonymous and eccentric lake (positioned collaterally) towards the enemy's objectives. In order to diminish the vulnerability of Constanţa in the face of a Russian maritime attack, M. Ionescu Dobrogianu proposed, in 1904, following the Danish model of the fortified island in front of Copenhagen, the installation of a coastal battery and the establishment of a defence pier, the fortification on land being considered useless[43]. In fact, Constanţa's vulnerability to the Russian fleet would be revealed in the following year, in the context of the famous episode of the cruiser Potemkin[44].

In the event of a Russian attack from the north, the same M. Ionescu Dobrogianu recommended the fortification of the Eski-Kalé part, considered more exposed, the surveillance of the Russian-speaking Lipovan population from the Delta, the installation of a torpedo battery on the Tulcea promontory and a torpedo dam at Ceatal, then the successive resistance to Babadag (on a short term), later to Hârşova, where it was recommended to build a bridge over the Danube (it would only be accomplished in 1966-1970). Once Hârşova and Isaccea were lost, resistance in the Cernavodă area became useless[45].

In the *"Report on the concentration of the army in hypothesis A"* (war against Russia), elaborated in December 1909 by Colonel Ioan Popovici, the 5th Army Corps had the mission to supervise the Cernavodă Bridge; the optimal concentration zone of the Romanian troops was located in the northeast of Walachia and the south of Moldavia on the right side of the Prut, so that, among others, to be close to Basarabia, Transilvania and Dobrogea[46].

[42] *Ibid*, p. 403-404.
[43] M. Ionescu Dobrogianu, *op. cit.,* p. 922.
[44] A. Rădulescu, I. Bitoleanu, *op. cit.*, p. 404.
[45] M. Ionescu Dobrogianu, *op. cit.*, pp. 919-921.
[46] Romanian National Military Archives – Military Archive Centre Pitești (RMNA – CADP), Great General Staff (GGS) Collection – Section 3 Operations, file 29/1909, rows 1-9.

In case of a Bulgarian ground attack on the Romanian Dobrogea, Captain M. Ionescu Dobrogianu wrote, in 1904, about the difficulty to find an optimal line of defence. As the most likely target of the Bulgarian attack was the Cernavodă bridge, the mentioned officer recommended organising two successive lines of defence, both located south of the Carasu Valley, namely the line delimited by the Urluia and Borungea valleys, with the centre at Enigea, respectively the line of the Peştera and Ikingi-Deré, with the centre at Medgidia[47]. Moreover, in the autumn 1916 campaign, the Romanian troops were withdrawn from Dobrogea, after losing the Constanţa-Cernavodă strategic line[48]. In a nationalistic brochure, published in 1919, Colonel Ion Antonescu observed that the disembarkation of enemy troops at Zimnicea, in November 1916, was carried out only after the Cernavodă-Constanţa line had been reached in Dobrogea[49].

Even today, the possibilities of fortification of the Dobrogea area are significantly influenced by the climate of the province. Thus, the torrential character of the rainfall, generally reduced in frequency, may trigger floods and landslides, with direct effects on the land, logistic transports or troops manoeuvre[50].

Going back to the Romanian-Bulgarian rivalries from more than a century ago in Dobrogea, we mention that during the period of great tension of 1900-1902 (after Professor Ştefan Mihăileanu's assassination)[51], the Romanian Great General Staff permanently received information about the movements of Bulgarian and Russian warships at the Black Sea[52]. In fact, in 1900, the construction of the bridgehead from Cernavodă was initiated, an operation that lasted until 1912, with the purpose of facilitating the operations of the Romanian army in Dobrogea and in the eastern sector of the Romanian Plain. The Russian government strongly protested against these actions, considered contrary to the provisions of Article 52 of the Berlin Treaty, but maintained a silent attitude towards similar actions by Bulgaria[53]. In 1903, General Constantin Christescu (1866-1923) drafted hypothesis C, in the eventuality of a Bulgarian attack on Romanian territory[54].

At the beginning of the 20th century, the Directorate General of State Security identified many Bulgarian officers crossing the border on the pretext of buying

[47] M. Ionescu Dobrogianu, *op. cit.*, p. 924.
[48] A. Rădulescu, I. Bitoleanu, *op. cit.*, p. 386.
[49] Ion Antonescu, *Românii – originea, trecutul, sacrificiile şi drepturile lor*, edited by Valeriu Florin Dobrinescu, Editura Moldova, Iaşi, 1991, p. 75.
[50] Valentin Dragomirescu, *Dobrogea: o analiză geografico-militară*, Editura Universității Naționale de Apărare *"Carol I"*, București, 2015, pp. 29-31.
[51] *I.P.E.R.D.*, pp. 200-201.
[52] G. Preda, *op. cit.*, p. 117.
[53] *Ibid*, pp. 113-115.
[54] P. Otu, *op. cit.*, p. 152 (Details in RMNA – CADP, GGS Collection – Section III Operations, file 10, passim).

necessary materials for the Bulgarian army (hay, firewood etc.) and trying to establish ties with Bulgarian ethnic groups in Romania and spy on military objects[55]. Also, the Romanian secret services had information on the training of Bulgarian gangs by the officers from the neighbouring country, in order to carry out espionage missions, including for the benefit of the Russian army[56].

Analysing the possibility of a war with Bulgaria, the Romanian decision-makers in this matter concluded that the Romanian state should not have the initiative for opening hostilities, but had to be prepared for offensive operations, the optimal solution of counteracting a Bulgarian attack in Dobrogea being the concentration of shock forces in Oltenia (Western Walachia), to threaten Sofia, the Dobrogea war-theatre playing a secondary role[57].

In 1908, the *"Report on the concentration of the Romanian army in hypothesis C"* (war against Bulgaria) was drawn up. The army of the neighbouring state was considered superior in terms of infantry and artillery, but inferior in terms of cavalry. After reviewing a series of drawbacks of the concentration of the Romanian troops in Dobrogea, the author of the memo concludes that: *"the line of operation of the Romanian army through Dobrogea puts the Bulgarians in such good conditions that, after all, victory can become theirs".* Even in the event of a rejection of the Bulgarian troops and a future pursuit, they had possibilities of strengthening on their own territory[58]. Starting from the reality of the Bulgarian political-territorial ambitions in the southeastern Europe, amplified after gaining full independence, in October 1908, Romanian Colonel Ioan Popovici drew up a homonymous version of hypothesis C, in 1910. According to Colonel Ioan Popovici, for the Romanian state and its army, the war could only be offensive, in order not to allow Bulgaria to gain the upper hand. After mentioning *"the too big difficulties that are foreseen in reaching an effective result, adopting the offensive through Dobrogea"*, he formulated the solution of an attack (march) towards Sofia, starting from the Danube Plain[59].

In the context of preparations for the coalition war against the Ottoman Empire (the first Balkan war), Serbia and Bulgaria concluded a military convention in the spring of 1912 that also stipulated a (defensive) war against Romania. In such a situation, Dobrogea was considered as the possible theatre of military operations, as was the Middle Danube or the Serbian territory[60].

[55] G. Preda, *op. cit.*, p. 125.
[56] *Ibid*, p. 126.
[57] P. Otu, *op. cit.,* p. 153.
[58] RMNA – CADP, GGS Collection – Section III Operations, file 23/1908, rows 20-36.
[59] *Ibid*, file no. crt. 28/1910, rows 1-8.
[60] D. Buşă, *op. cit.*, p. 246.

On the eve of Romania's intervention in the Second Balkan War, on 17 June 1913, General Alexandru Averescu finalised a *"Memorandum regarding the guidance of the Romanian army's operations in case of intervention in the Serbian-Bulgarian conflict"*. The future Romanian Marshal appreciated that *"the line of operations that presents the most advantages for advancing the main forces is the cluster that starts from the Danube, in front of Bechet-Corabia-Turnu Măgurele points"*[61]. In fact, in the short summer 1913 campaign, Romania's main operations army concentrated on the left bank of the Danube, under the leadership of Crown Prince Ferdinand, later crossing the river, on the Bulgarian territory, while the Romanian Dobrogea represented the starting point for the Dobrogea Corps offensive, under the command of General Ioan Culcer[62].

As the possibility of a substantial territorial expansion of Bulgaria on the part of the Ottoman Empire, especially in Macedonia, became increasingly clear in the Romanian political, diplomatic and military circles, the idea of a proper territorial compensation of the Romanian state appeared. The northeastern areas of the Bulgarian state, up to the Silistra-Varna or even Rusciuk-Varna lines, were considered as a strategic cover of the territory obtained in 1878; what the promoters of these ideas underestimated or ignored was the extent of the changes in Southern Dobrogea, after 1878, to the benefit of the ethnic Bulgarians (and to the disadvantage of the Muslims), both in terms of demographics and, above all, of economic-social relations. The Romanian plans to push south of the land border with Bulgaria, in case of the collapse of the Ottoman rule in the Balkans, were unsuccessfully communicated in Vienna and Berlin, in January 1901 by P.P. Carp[63], then by Ion I.C. Brătianu; in September 1909[64], but also in Sofia, in 1902, by King Carol I himself[65].

The territorial expansion of the Romanian state to the south of Dobrogea was to take place under the conditions of the second Balkan war, in the summer of 1913. The territory acquired then, called *Quadrilateral*, due to its almost quadrangle form, *Southern Dobrogea*, or *New Dobrogea* (in opposition to *Old Dobrogea*, which is part of Romania since 1878), did not prove to be a true strategic cover of the Cernavodă-Constanţa line, neither during the years of the First World War nor during the two interwar decades[66]. In addition, the administration of the Quadrilateral

[61] D. Preda, E. Ardeleanu, Al. Oşca, *op. cit.*, p. 67.
[62] P. Otu, *op. cit.,* p. 160.
[63] *I.P.E.R.D.*, p. 201.
[64] K. Hitchins, *op. cit.*, pp. 154-155.
[65] Gh. A. Dabija, *Amintirile unui ataşat militar român în Bulgaria (1910-1913)*, Tipografia *"Universul"*, Bucureşti, 1936, p. 163; H. Hesapciev, *op. cit.*, pp. 17-18.
[66] G. Ungureanu, *op. cit.*, pp. 67-75.

posed many and difficult problems to the Romanian administration, some of them also affecting the international relations level[67].

At the time of annexing (northern and central) Dobrogea under the Romanian state jurisdiction, the agriculture of this province was burdened, on the one hand, by the Ottoman inheritance in the field of financial law, and on the other hand, by the restricted share of the cultivated land in relation to the uncultivated ones (ponds, marshes etc.).

An essential feature of the Ottoman land tenure system was the placing of the most extensive arable land in the *Mirie* category, i.e. not in the full ownership of the cultivators, but only in their hereditary use, revocable in case of repeated non-cultivation of the land entrusted by the state, personified by the sultan. The Laws on Dobrogea issued by the Romanian authorities in 1880 and 1882 stipulated the transformation of the *Mirie* type properties into full private properties, in exchange for the payment of staggering amounts over 15 years. The Law of 1884 stipulated the rescheduling of the respective amounts for 20 years, in parallel with the alternative possibility of assigning a third of the *Mirie* surfaces, in exchange for the recognition of the full property right over the rest for the owners[68]. As a result of the confiscations of *"thirds"* and other legal measures, the Romanian state acquired a total of 165,142 hectares (127,843 in Constanţa county and 37,309 in Tulcea county), representing about 1/9 of the Romanian Dobrogea area. Of this total, 60,552 hectares remained state property, and the rest (almost 2/3) was distributed to the native population or to the colonists brought to the area[69].

Much more than from confiscations, the Romanian state increased its Dobrogea land reserve following the works of enhancement of the territory (remedies, desiccations, divisions, deserts etc.). Thus, between 1884 and 1905, the cultivated area of the Romanian Dobrogea increased from 240,000 hectares to over 800,000 hectares[70]. The works in question also contributed to the improvement of the hygienic-sanitary state, the ponds and marshes representing a favourable environment for a wide range of bio-pathogens[71].

The cumulative result of the constructive and coercive-state measures, applied by the Romanian authorities in Dobrogea, in the land domain, constituted a solid basis for the redistribution of property, through sale-purchase. Until 1908,

[67] *Ibid, passim*.
[68] Ioan N. Roman, *Proprietatea imobiliară rurală în Dobrogea*, in vol. *Dobrogea – 50 de ani de viaţă românească (1878-1928)*, manager: C-tin Brătescu, secretary: I. Georgescu, Cultura Naţională, Bucureşti, 1928, pp. 285-286.
[69] Toma Ionescu, *Asupra proprietăţilor şi colonizărilor în Dobrogea*, in *Dobrogea – 50 de ani…*, p. 278.
[70] Gheorghe Iacob, *Repere ale evoluţiei economice*, in *Istoria românilor* (academic treatise), tome VII, T2; *De la Independenţă la Marea Unire (1878-1918)*, coord.: acad. Gh. Platon, Editura Enciclopedică, Bucureşti, 2003, p. 167.
[71] M. Ionescu Dobrogianu, *op.cit.*, p. 204.

the Romanian state sold a total of 400,452 hectares of Dobrogea arable land, of which about 2/3 (260,163 ha.) to Romanian ethnic groups (colonists or natives), and 140,379 to Romanian citizens of other ethnicities[72]. Meanwhile, in 1903, a law of ownership for those who fought in the War of Independence (1877-1878) was issued, according to which they were granted 2000 m2 of home fireplace, plus lots of 8 hectares, in exchange for amounts payable in 60 years annuities; in addition, they benefited from a five-year tax exemption and aid for building houses and purchasing cattle and agricultural tools, as well as fruit trees and nozzles from state nurseries[73].

However, the yield of the plant crop was low, compared to the rest of the country, a fact that can be explained either by the smaller proportion of the plows (24 to 100 hectares, compared to 36 in Moldavia and Walachia[74]), or by the dependence on the very fluctuating climatic conditions[75].

A well-represented branch of activity in the pre-war Romanian Dobrogea was animal breeding. Thus, at the beginning of the last century, the province sheltered the eighth part of Romania's sheep and goats flocks; the number of sheep per capita of Dobrogea (3) was higher than any country in Europe (Greece – 2.5, Bulgaria – 2, Serbia – 1.5 etc.). In 1904, in Constanţa and Tulcea counties, a horse was registered to 2.7 respectively 3 inhabitants, a large horn to 1.38, respectively 2.44 inhabitants, a small horn to 3.7, respectively 1.2 inhabitants, a pig to 6, respectively 5.8 inhabitants[76].

Due to the specific conditions and measures taken by the central and local authorities, Dobrogea was not affected by the peasant movements that shook the Old Kingdom of Romania between 1888 and 1907.

If the industrialisation itself made little progress in Dobrogea from 1878-1913, not the same can be said about communications and commerce. An important stage for the connection of Dobrogea with the rest of the Romanian territory is represented by the years 1890-1895, when we note the establishment of the Romanian River Navigation (1890), then of the Romanian Maritime Service (1895), almost simultaneously with the inauguration of the Cernavodă bridge[77]. In fact, the building of the Bucharest-Feteşti railway line and a trans-Danube bridge had been stipulated in a law adopted in June 1882, and three years later, the construction of the bridge over the Danube and the reconstruction of Constanţa port were declared works of public utility, following a few years of failed auctions[78].

[72] Marin Vlădescu-Olt, *Constituţia Dobrogei*, Tipografia "Doru P. Cucu", Bucureşti, 1908, pp. 131-132.
[73] A. Rădulescu, I. Bitoleanu, *op. cit.*, pp. 358, 370.
[74] M. Ionescu Dobrogianu, *op. cit.*, p. 935.
[75] A. Rădulescu, I. Bitoleanu, *op. cit.*, p. 371.
[76] *Ibid,* p. 796.
[77] Gh. Iacob, *Repere ale evoluţiei economice…* , p. 120.
[78] M. Ionescu Dobrogianu, *op. cit.*, p. 676.

In 1887, the Ministry of Public Works gave up the idea of a tender, setting up a special service, under the guidance of engineer Anghel Saligny (b. 1854-d. 1925), who, assisted by other Romanian engineers, drew up a project, finalised and accepted in the year 1889, when the actual works began[79]. After six years, Dobrogea was linked to Walachia, in the Feteşti-Cernavodă area, by the longest bridge complex in Europe and the second in the world[80]. Between Cernavodă and Constanţa, a railway line had been built, is the Ottoman period (1857-1862), by a British company[81]. Tulcea County, not connected to the rest of Dobrogea (and the country) by rail, would have a slower development than Constanţa[82]. Dobrogea road network was represented, in 1900, by two national roads (Constanţa-Babadag-Tulcea and Tulcea-Ghecet), 41 neighbourhood roads and 9 communal roads[83].

After the repurchase from the British company *"Danube and Black Sea Railway and Küstenge Harbor Company Ltd."* (the same one that built the Constanţa-Cernavodă railway), the modernisation of the port of Constanţa started on 16 October 1896, being entrusted to the French company Hallier, and after its bankruptcy (1899), to the engineer Anghel Salingny[84].

Also in 1899, the direct railway line Berlin-Constanţa was inaugurated, and six years later the Constanța-Istanbul[85] submarine cable was used, the metropolis of Northern Dobrogea becoming a nodal point between Central Europe and the Near East. On 27 September 1909, in the presence of the royal family and the members of the government, the celebrations of the inauguration of the port of Constanţa took place, occasion on which, symbolically, the ship *"Iași"* was loaded with cereals for export, from the first warehouse-silo built by A. Saligny, who was also present at the event[86].

Between 1889 and 1913, the volume of trade practised in the port of Constanţa increased from 89,400 tones to 1.5 million tones, representing one-third of the total export of Romania since then, including 85% of the quantity of oil exported. Currently, through the port of Constanţa pass about 15 million tons annually[87]. Going back to the nineteenth and twentieth centuries, we also mention that during this period, about 90% of the volume of Romanian foreign trade was carried out

[79] A Rădulescu, I. Bitoleanu, *op. cit.*, p. 367.
[80] V. Dragomirescu, *op. cit.*, p. 192.
[81] *Ibid*, p. 168.
[82] A. Rădulescu, I. Bitoleanu, *op. cit.*, p. 369.
[83] M. Ionescu Dobrogianu, *op. cit.*, p. 684.
[84] V. Dragomirescu, *op. cit.*, p. 169.
[85] A. Rădulescu, I. Bitoleanu, *op. cit.*, pp. 402-403.
[86] *Ibid*, p. 403.
[87] V. Dragomirescu, *op. cit.*, p. 39.

with the western states (including Austro-Hungary), 8% with the Balkan states (including the Ottoman Empire) and only 2% with the Russian Empire[88].

A third of a century after joining Romania, Dobrogea became the most urbanised province, among the four of the Old Romanian Kingdom, with a share of the city population of 25%, compared with less than 10% in Oltenia (Western Wallachia), 18% in Moldova and about 22 % in Muntenia (Eastern Walachia), thanks to the Capital (country average: 18.4%)[89].

The actions of the Romanian authorities to make the most of the Dobrogea territory and to state some agricultural lands, in conjunction with the development of communication routes, created a solid basis for the colonisation process of the province between the Danube and the Sea. Not unimportant is the fact that, after the use of the Cernavodă Bridge, the colonisation experienced a significant acceleration[90]. In turn, the colonisation considerably transformed the ethno-demographic structure of the province between the Danube and the Sea. Thus, in 1913, *Old Dobrogea* had a total population of 384,420 inhabitants (over 2.5 times more than in 1880), of which 209,571 in Constanţa county and 170,859 in Tulcea county[91]. The Romanian ethnic groups made up the absolute majority of the population (216,425 inhabitants, 56.9%), their share being slightly higher in Constanţa county compared to Tulcea (61.6%, compared to 51.1%). The second place was the Bulgarian ethnic group, 51,149 (13.4%), followed by the Turks-Tartars (41,442 inhabitants or 10.9%). The Russians and the Lipovans, 35,849, represented 9.4% of the population, and the 9,999 Greeks made up 2.6% of the total population[92].

Of the more than 200,000 Romanians from *Old Dobrogea*, recorded in 1913, only a quarter (24.2%) were *dicieni* (Romanians who were there in 1878 or their descendants), while 39.5% were *cojani* (from the plains of Walachia, 21.8% were *mocani* (coming from Transylvania and Banat, under Hungarian domination), 8% were Moldovans from the right bank of the Prut, and 5.6% were Romanians from Basarabia[93]. One should notice as well the significant increase of Romanians in Tulcea county, between 1908 and 1913, from about 40% (62,204 out of 154,147)[94] to 51[95]. An area with a significant share of the non-Romanian population remains

[88] G. Preda, *op. cit.*, pp. 115-116.
[89] Veličko Georgiev, Stajko Trifonov (editors), *Istorija na Bălgarite (1878-1944) v dokumenti,* Tom I, 1878-1912, Prosveta, Sofia, 1996, p. 561.
[90] M. Ionescu Dobrogianu, *op. cit.*, p. 931.
[91] A. Rădulescu, I. Bitoleanu, *op. cit.,* p 360.
[92] *Ibid*.
[93] Constantin Iordache, *Rumînskata Kalifornija: integriraneto na Severna Dobrudža v Rumînija (1878-1913)*, in *"Istoričeski Pregled"*, 57, nr. 3-4/2001, p. 63.
[94] Romulus Seişanu, *Dobrogea, Gurile Dunării şi Insula Şerpilor*, Tipografia *"Universul"*, Bucureşti, 1928, p. 193.
[95] See *supra*, notice 97.

the Danube Delta, where Prefect Ioan Neniţescu had tried, at the end of the 19th century, to initiate a colonising action[96]. The share of Romanian ethnicities had increased not only demographically, but also socially-economically, being relevant in this regard the fact that Dobrogea was the only province of the Old Kingdom since 1912 where they were better represented in the urban environment than in the rural one (80.45%, compared to 48.2%)[97].

As we have seen, the Bulgarians registered a decrease of one-third of the demographic share (from 19.9 to 13.4 percent), but, in absolute numbers, their number saw a significant increase, from about 30,000 to over 51,000, representing an increase of 70% over 33 years (1880-1913). According to some Romanian sources, this increase was due to the Bulgarian immigrants from Southern Basarabia, caused by the revocation by the Czarist authorities of the privileges granted at the beginning of the 19th century to the Bulgarian colonists[98]. The share of Bulgarian ethnicities in the rural economic and social life of the province remained, after all indications, higher than the demographic itself. A statistics from 1906, put into circulation by Vasile M. Kogălniceanu and used by Bulgarian propagandist Ivan St. Penakov, in the interwar years, recorded, on the territory of Tulcea county, a total of 9,742 Romanian agricultural households, totalling 97,000 hectares (on average, about 10 hectares per household), respectively 5,794 Bulgarian agricultural households, totalling 85,504 hectares (on average, about 15 ha per household)[99]. The deputy of Macedonian-Romanian origin, Achile Pinetta showed, in the parliamentary sitting of 8 April 1922, without being contradicted by auditors or other speakers, that the Bulgarian ethnic groups from Northern Dobrogea had succeeded in taking advantage of the opportunities offered by the stipulations of the Romanian land regime, having documents of property and sufficient financial reserves not only for the payment of fees for the transformation of *Miri*e properties into full private property, but also for the acquisition of land[100].

Despite the good relations with the Romanian authorities on the political and cultural level, the situation of the Turkish Tartars experienced a significant economic and social degradation. Their number, in absolute numbers, remains the same, but the demographic percentage share drops almost three times, between 1880 and 1913, from 31% to 11%, while the arable area held was reduced to no more than one-

[96] M. Ionescu Dobrogianu, *op. cit.*, pp. 268-269.
[97] Răzvan Limona, *Populaţia Dobrogei în perioada interbelică*, *Semănătorul*, online publishing, August 2009, Tulcea, p. 26, the text is available at tulcealibrary.com, retrieved on 29.08.2019.
[98] Central National Historical Archives of Romania, *Presidency of the Council* of *Ministers* Collection, file no. 131/1939, rows 31-32.
[99] *Apud* Ivan St. Penakov, *L'entente bulgaro-roumaine. Premisses*, Editura T.F. Tchipeff, Sofia, 1939, pp. 20-21.
[100] *"Monitorul Oficial – Dezbaterile Adunării Deputaţilor",* no. 20 of 30 April 1922, sitting of 8 April 1922, in *Sesiunea ordinară 1921-1922*, Imprimeria naţională, Bucureşti, 1922, p. 347.

sixth; several socio-cultural factors contributed to this dramatic involution: lack of an Ottoman tradition of written acts, language barrier, Islamic conservatism, but also certain attitudes and behaviours of Romanian officials[101]. The precariousness of the living conditions of the Dobrogea Muslims also made its mark on the degree of literacy (very low, although the two counties occupied, in 1912, the 2nd and the 3rd places among all the 32 counties of the Old Romanian Kingdom, in this chapter)[102], "as and hygiene-sanitary condition, their homes being considered *"true outbreaks of infection"*[103].

When it became part of the modern Romanian national state (1878), the northern and central Dobrogea territory was considered by the Romanians as an area of maximum vulnerability, for multiple reasons (Trans-Danube position, ethno-demographic composition, precarious economic situation, etc.). The main fears were related to the affinities and connivances between Russia and Bulgaria. In order to safeguard and strengthen its sovereignty in Dobrogea, the Romanian state has taken a series of measures, both at the political and military level, and at the ethnopolitical level (i.e. economic, social, cultural ones, etc.). The actual military measures (the establishment of the Danube Division and the Great Division), the deployment in the area of the 5th Army Corps, the building of the bridgehead from Cernavodă, etc.), affected by a whole series of difficulties and objective deficiencies, offered limited results, but Romania's security options and European pre-war balance made up for this disadvantage. A remarkable success was the measures of the second category (the enhancement of the territory, the development of the communication routes and the port of Constanţa, the colonisation etc.), in their essence, of constructive-integrative type and only occasionally of coercive type. These led to the full integration of Dobrogea into the Romanian national-state edifice, a process that will prove irreversible, in the context of affirming the principle of national self-determination and under the conditions of the Romanian foreign policy option since August 1916.

BIBLIOGRAPHY

1. ***, *Istoria militară a poporului român*, vol. V (1878-1919), Editura Militară, Bucureşti, 1988.
2. ***, *Istoria politicii externe româneşti în date*, coord.: Ion Calafeteanu, Editura Enciclopedic, Bucureşti, 2003.

[101] M. Ülküsal, *Dobruça ve Türkler,* Turkish Institute for Culture and Researches, Ankara, 1966, pp. 24-44.
[102] A. Rădulescu, I. Bitoleanu, *op. cit.,* p 394.
[103] M. Ionescu Dobrogianu, *op. cit.*, p. 61.

3. ***, *Istoria românilor* (academic treatise), vol. VII, T1; *Constituirea României moderne (1821-1878)*, 2nd edition revised and added, coord.: acad. Dan Berindei, Editura Enciclopedică , Bucureşti, 2015.
4. ***, *Istoria românilor* (academic treatise), vol. VII, T2; *De la Independenţă la Marea Unire (1878-1918)*, coord.: acad. Gh. Platon, Ed. Enciclopedică, Bucureşti, 2003.
5. ***, *La Dobroudja*, edité par l'Union de savants, artists et ecrivains bulgares, Sofia, 1918.
6. ***, *Monitorul Oficial – Dezbaterile Adunării Deputaţilor*, no. 20 of 30 April 1922, sitting of 8 April 1922, in the volume *Sesiunea ordinară 1921-1922*, Imprimeria Naţională, Bucureşti, 1922.
7. ***, *Novi očerci po bălgarskata istorija (1878-1948)*, săstavitel Marija Radeva, f.ed., Sofija, f.a.
8. Arhivele Militare Naţionale Române/Romanian National Military Archive – Military Archive Centre (Piteşti), *Great General Staff* Collection, 3rd Operations Section, files 10, 12, 17, 23, 24, 28, 29.
9. Central Historical National Archives, *Presidency of the Council of Ministers* Collection, file no. 131-1939.
10. Ion Antonescu, *Românii, originea, trecutul, sacrificiile şi drepturile lor*, edition by Valeriu Florin Dobrinescu, Editura Moldova, Iaşi, 1991.
11. Constantin Brătescu, *Monografia Cadrilaterului*, Cernăuţi, 1938.
12. Daniela Buşă, *Modificări politice şi teritoriale în sud-estul Europei (1878-1914),* Editura Paideia, Bucureşti, 2003, pp. 48-57.
13. Valentin Ciorbea (coord.), *Dobrogea (1878-2008). Orizonturi deschise prin mandat european*, Editura EX PONTO, Constanţa, 2008.
14. Gheorghe A. Dabija, *Amintirile unui ataşat militar român în Bulgaria (1910-1913),* Tipografia ziarului *"Universul"*, Bucureşti, 1936.
15. Sorin Liviu Damean, *România şi Congresul de Pace de la Berlin (1878),* Editura Mica Valahie, Bucureşti, 2011.
16. *Dobrogea: 50 de ani de viaţă românească (1878-1928),* Director: Constantin Brătescu, Secretary: I. Georgescu, Cultura Naţională, Bucureşti, 1928.
17. Valentin Dragomirescu, *Dobrogea: analiza geografico-militară*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2015.
18. George Ene, *Eminescu, securitatea şi siguranţa naţională a României*, Editura Eikon, Cluj-Napoca, 2014.
19. Veličko Georgiev, Stajko Trifonov (săstaviteli), *Istorija na Bălgarite (1878-1944) v dokumenti",* Tom I, 1878-1912, Prosveta, Sofija, 1996.
20. Hristofor Hesapciev, *Amintirile unui fost diplomat bulgar în România (1905-1910),* traducere de Daniel Cain, Editura Fundaţiei PRO, Bucureşti, 2003.
21. Keith Hitchins, *Românii (1866-1947),* 3rd edition, translated by George G. Pora and Delia Răzdolescu, Editura Humanitas, Bucureşti, 2004.
22. Dobrogianu Marin Ionescu, *Dobrogea în pragul veacului al XX-lea. Geografia matematică, fizică, politică, economică şi militară*, Atelierele Grafice Socec, Bucureşti, 1904.
23. Constantin Iordache, *Rumînskata Kalifornija: integriraneto na Severna Dobrudža v Ruminija (1878-1913),* in *Istoričeski Pregled*, 57, no. 3-4/2001.

24. Constantin Iordan, *Dobrogea (1878-1940) în istoriografia bulgară post-comunistă*, Editura Academiei Române, 2013.
25. Constantin Iordan, *România şi relaţiile internaţionale în sud-estul european (1919- 1924). Probleme ale păcii, securităţii şi cooperării*, Editura ALL, Bucureşti, 1999.
26. Antonina Kuzmanova, *Le caractére bulgare de la Dobrodja vu par les Roumains. Propagande et mire en comideration des réalités (1878-1944),* in *"Etudes balkaniques",* 29, nr. 31, 1993.
27. Limona Răzvan, *Populaţia Dobrogei în perioada interbelică*, *Semănătorul*, online publishing house, Tulcea, August 2009, available at tulcealibrary.com, retrieved on 29.08.2019.
28. William Miller, *The Ottoman Empire and its Succesors (1801-1927),* Cambridge, 1927.
29. Ioan Munteanu, *Cadrilaterul, istoria unei controverse (1878-1919),* in *Anuarul Institutului pentru Studii Politice de Apărare şi Istorie Militară*, Bucureşti, 1997.
30. Blagovest Njagulov, *Les images de l'autre chez les Bulgares et les Roumaines (1878- 1944),* in *Etudes balkaniques*, 31, nr. 2/1995.
31. Stevan K. Pavlowitch, *Istoria Balcanilor (1804-1945),* translated by Andreea Doica, Editura Polirom, Iaşi, 2002.
32. Ivan St. Penakov, *L'entente bulgaro-roumaine. Premisses*, Imprimerie T.F. Tchipeff, Sofia, 1939.
33. Žeko Popov, *La situation et les luttes des Bulgares de la Dobroudja de Nord (1878- 1913),* in *"Bulgarian Historical Review"*, 19, nr. 1/1991.
34. Joseph V. Poppov, *La Dobroudja et les relations bulgaro-roumaines*, Liège, 1935.
35. Dumitru Preda, Alexandru Oşca, Eftimie Ardeleanu, *Proiecte şi planuri de operaţii ale M.St.M. Român (până în anul 1916),* edited by the Romanian Military History Commission, Bucureşti, 1992.
36. Adrian Rădulescu, Ion Bitoleanu, *Istoria Dobrogei*, 2nd edition, Editura EX PONTO, Constanţa, 1998.
37. Florin Anghel, Mariana Cojoc, Magdalena Tiţă coord., *Români şi bulgari. Provocările unei vecinătăţi*, Editura Cartea Universitară, Bucureşti, 2007.
38. Romulus Seişanu, *Dobrogea, Gurile Dunării şi Insula Şerpilor*, Tipografia *"Universul"*, Bucureşti, 1928.
39. Robert Stănciugel, Liliana Monica Bălaşa, *Dobrogea între secolele VII-XIX. Evoluţie istorică*, Editura D.C. Promotions, Bucureşti, 2005.
40. George Ungureanu, *Problema Cadrilaterului în contextul relaţiilor româno-bulgare (1919-1940)*, Editura Istros, Brăila, 2009.
41. Müstecib Ülküsal, *Dobruça ve Türkler*, Aratşirma Türk Kültürnii Enstitutu, Ankara, 1966.
42. Marin Vlădescu-Olt, *Constituţia Dobrogei*, Tipografia "Doru P. Cucu", Bucureşti, 1908.
43. Gheorghe Zbuchea, *România şi războaiele balcanice (1912-1913). Pagini de istorie sud-est europeană*, Editura Albatros, 1999.

THE CONCEPTION OF THE ARMED FORCES GENERAL STAFF REGARDING THE DEFENCE OF DOBROGEA AT THE BEGINNING OF THE 20TH CENTURY

ION RÎŞNOVEANU, PhD

Scientific Researcher III, "King Ferdinand I" National Military Museum

At the start of the twentieth century, the Romanian General Staff was busy constructing Romania's defence doctrine. They were focused on the most probable situations, in which Romania would be forced to defend itself.

The officers of the General Staff used reports from the military attachés in Petersburg and Sofia and identified that Dobrogea was targeted by two potential aggressors – Russia and Bulgaria.

This is why the planners made detailed drafts to those defence plans, focusing on the different defence lines from the Danube Delta to the Black Sea Coast, in the case of a Russian aggression. For southern Dobrogea, a delicate area after the Peace of Bucharest in 1913, after which Romania received the counties of Durostor and Caliacra (or Quadrilateral, as it appears on Romanian military maps) new alinements were viewed as essential for the defence of the area against the Bulgarians.

Keywords: World War I, Romanian Army, military doctrine, military attachés, defence line.

THE FIRST MILITARY MEASURES TAKEN BY THE GENERAL STAFF OF THE ROMANIAN ARMY FOR THE DEFENCE OF DOBROGEA AT THE BEGINNING OF THE 20TH CENTURY

From the study of the specialised literature, it can be concluded that the *doctrine consists in deducing a certain number of principles, corroborated with the development on the map or on the field of a significant number of concrete cases and, thereafter, by making these principles enter into the blood of everybody.* Thus, *all officers will work in the same way, because they will be guided by the same principles*[1]. By extension, the military doctrine was appreciated as a *science, erudition, learning […] principle, conduct rule*[2], actually being *the life of an army, its moral force*[3].

Studies during 1878-1913 have shown that, from a military point of view, Dobrogea, without Silistra and its fortified positions, represented a burden for the defensive system of modern Romania which needed engineering works and concentrations of forces that would have weakened the defence excentered to multi-area concept[4]. Still, even in these conditions, the General Staff of the Romanian Army was conceiving the organisation of the defence of the country's territorial integrity in a unitary system in which Dobrogea played the role of a strategic outpost that would be tested within a large-scale military confrontation, the military potential of the army and the Romanian state[5].

Before the First World War, in the conception of the General Staff of the Romanian Army, South Dobrogea was considered as a possible area of concentration of the Bulgarian army and as an alignment of departure to its offensive in case of an aggression on the land between the Danube and the Black Sea[6].

The defence of Dobrogea was conceived by the Romanian General Staff, by arranging in covering the border, besides the existing Great Units, the guards,

1 *Revista Armatei*, year XII, October, 1895, p. 782.
2 *Revista Infanteriei*, year XVIII, July-August 1914, p. 56.
3 *România Militară*, year XIII, December 1896, p. 355.
4 Locotenent-colonel Ioan Munteanu, *Cadrilaterul – istoria unei controverse*, in "*Anuarul de studii de politică de apărare şi istorie militare*", Editura Pro Transilvania, Bucureşti, 1997, p. 185.
5 Romanian Military Archives/Arhivele Militare Române (AMR), *Microfilms* Collection, P.II 1922, c. 418.
6 Romanian National Archives/Arhivele Naţionale Române (ANR), *Royal Family* Collection, vol. I, file no. 2/1913, ff. 2-12.

infantry and cavalry troops, with missions of surveillance and reconnaissance. A first defence position, with relatively insular character, included the fortified alignments Turtucaia, Silistra and Bazargic, located in space at appreciable distances, measuring in a straight line 113 km, along the front. The second position passed on the alignment located towards the central part of the South Dobrogea plateau towards Canlia (immediately in the North-West of the Bugeac lake) and Mangalia, while the third position followed the alignment Rasova, Cobadin, Topraisar. Finally, the second position included *the bridgehead* from Cernavoda, then it continued on Medgidia-Agigea alignment.

At the beginning of the 20th century, in the opinion of some military researchers, such as Colonel Marin Ionescu-Dobrogeanu, the defence of Dobrogea, at least in front of an attack that would have come from the South or from the sea, had major deficiencies. Therefore, a good connoisseur of the realities in the field, the famous military historian proposed a more economical and effective border guard system. Field organisation at the end of the 20th century, as regards to the defence of the Southern border of Dobrogea, was assigned to eight permanent and non-permanent infantry companies unevenly spread over a distance of 131 km. These were positioned at certain pickets that scrutinised the border line irregularly, the distances between them being quite large, without means of connection. Moreover, the rugged landscape in the area was an appropriate factor that further limited the effectiveness of the defence. Thus, a permanent battalion was placed at Ostrov, with three deployed companies in this locality, and one in Asarlîc, at no less than 69 km distance from the border. If the border guard in the immediate neighbourhood of the above-mentioned city up to picket 14 was rarely carried out by the soldiers of the three companies recalled, from picket 28 to Asarlîc, the disposition was insured by the 4th Company of the battalion. Intercalary, the pickets 22-28 were insured by another company of the 34th Infantry Regiment.

Summing up this sector, it turns out the 68,4 km were occupied by five companies, the biggest problem being that, apart from those of the 34th Infantry Regiment, the rest were non-permanent, the soldiers being mostly conscripted from the neighbouring villages, the majority being of Bulgarian ethnicity. The supply was poor, the valleys crossing the border were fallen, then, towards Danube, forcing the means of transport to make large detours. At the East of Asarlîc, towards Mangalia, the guard was carried out by other three companies, including the one from the seaside city. Again, a company of 34th Infantry Regiment interlaced with a company from the border during pickets 29-40, i.e. on a 37 km stretch. In Mangalia, the guard

service was carried out by a permanent company which provided five pickets, from 41 to 45, covering a distance of 27 km to the sea[7].

As Colonel Ionescu-Dobrogeanu noticed in his study, disadvantages of this system were the difficulties arisen in communication and supply among pickets that were due to adverse relief, the border being furrowed by valleys without arranged roads, this causing difficulties in changing people within the troop. It was also noted that, behind this picket line, there was no other establishment or concentration of forces to meet an enemy group or a small group that would have succeeded to pass by one of the border surveillance points. In this regard, it proposed a radial system for the deployment of the troops near the border, from which to reach easier to any point of surveillance on the Southern border, given that the two companies of the 34th Infantry Regiment should have been brought to Cuzgun and Enghez for training.

Also here should have been located the concentration centres for the two battalions in the composition of which the other companies deployed on the border entered. They would have surveyed the border divided almost equally, from Cuzgun on a radius of 67 km and from Enghez to the Black Sea on a radius of 64 km. The battalion from Cuzgun should have sent a company to Ostrov, deployed on a distance of 14 km, another to Cuiugiuk guarding the border on 12 km, the third at Parachioi on a length of another 19 km, the last having the sector of action also inside, at Asarlîc, having allocated 15 km of border.

The second battalion, from Enghez, had a company at Bairam-Dede to supervise an area of 16 km, the second at Caraormer on 21 km of border, the third at Sarighiol having to guard the border on 21 km, which the company deployed at Mangalia being assigned with the remaining 10 km to the seaside. Compared to the settlement in the field, a company was not assigned with more than 18 km compared to 36, as it was at that time. Moreover, thanks to the radial concentration system, the connection between the companies would have been achieved easier. In addition, the two centres could constitute a second line of defence behind the border.

It was also proposed the creation of a telephone line connecting the pickets and, in the future, it was necessary to conceive a plan to connect these points from the border with a modern and practical road.

[7] Marin Ionescu Dobrogeanu, *Dobrogea* în *pragul veacului al XX-lea,* Atelierele Grafice *"I.V. Socecu"*, Bucureşti, 1904, p. 913.

DOCTRINAL AND PRACTICAL PREPARATIONS FOR THE DEFENCE OF THE DANUBE LINE IN FRONT OF AN ATTACK FROM THE NORTH

In the opening of the analysis of the defence system and tactical plans of positioning and action in Dobrogea, depending on the attacks that could have come from the North, South and from the seaside, Colonel Marin Ionescu-Dobrogeanu performed an interesting metaphorical-anthropological resemblance of Dobrogea, describing it as a *trunk on which the body of our whole Country is resting*[8]. From the observations on the Russian-Turkish wars that took place in the 19th century, following the analysis of manoeuvres carried out by the great military formations of the two empires on the territory of Dobrogea, the author draws the general lines from which the value of this land arises when designing a strategic plan of operation in the Carpathian-Danubian-Pontic area. The importance of morphological formations present in Dobrogea, the fortress character impregnated by the province being bordered by the Danube River were elements to be taken into account when conducting a strategic analysis of the importance of territory in question.

As it can be seen from the same plastic comparison afore mentioned, … *the defence line Focșani-Nămoloasa-Galați is like a steel belt with which Major Schumann endowed our Country, this belt being useless, as long as we do not seek to keep the pillar trunk, Dobrogea, untouched…*[9]. The tendency of the countries to transform the Black Sea into a Russian lake in their march to Constantinople gave the Trans-Danubian province an increased importance in the wars they had against the Turks and their allies until 1877.

Because of this, the Russians crossed the Danube with the bulk of the troops in Dobrogea, not in Muntenia or Oltenia. Indeed, the 1854-1855 war was planned to take place in Dobrogea, where the Tsar's army had concentrated its bulk of troops and, most certainly, it would have happened if cholera had not intervened. The Russians direction of attack, in order to stop the important Romanian ally in a potential war with the Western Europe, would have been the elimination of Focșani-Nămoloasa line by a rear attack from Hârșova, but this would have not been possible without crossing the Danube from Gura Prutului to the Black Sea. Another observation of the illustrious Romanian strategist and historian was that, once arrived in Dobrogea, at the Danube mouths, the Russians would have cancelled the European Commission of Danube, so that, in these conditions, the defence

[8] *Ibid*, p. 915.
[9] *Ibid*.

of this province became a mission that was not only Romania's task, but the task of the entire Europe[10].

At the end of the 19th and early 20th centuries, Danube was the border of Dobrogea with Russia, on a length of 29,5 km, from Gura Prutului to Ceatal-Ismail. From here, the border followed the course of Chilia horn and the mouth Stari-Stambul to the Black Sea. Indeed, due to the width of the river up to 1,500 meters, on the first segment mentioned, it represented a serious obstacle that could hardly be overcome without careful engineering preparations. Moreover, the nature of Dobrogea shore is rocky, and behind the shores, the land, on a wide area, is marshy, leaving no firm ground to approach the riverbed[11]. In front of the passage that Russians would have tried at Reni there were the marshy lands of Cotul Pisica, an area with many large lakes. An attempt on Bugeacul hill would have been hampered by the heights on the Romanian shore, which are ideal points for positioning heavy artillery batteries. In front of the most possible crossing of Danube at Cartal and Teraponti, there was the important position of Isaccea, but here the river has a width of 1,000-1,250 m. From the heights between Isaccea and Rachel, the Russian troops would have been greeted by a rain of shells and bullets from the Romanian positions placed in this sector[12].

In this regard, Colonel Marin Ionescu-Dobrogeanu proposed to focus the attention of the military forces on the fortification in this point of the position from Eski-Kale. Another observation to be taken into account, made following the Russian campaign in Dobrogea in 1828, was the careful supervision of Russian population in the Delta.

Downstream of Isaccea, the river shores were not favourable to a mass crossing. The promontory on which the old city Tulcea was located, destroyed in 1828, was constituted in an ideal position for placing some Romanian powerful coastal artillery batteries to greet the Russian fleet that would attempt to go across the Danube. Lakes and marshes from the opposite shore made it even more difficult for the enemy. In order to defend the river against the enemy ships, at Ceatal it was proposed the building of a mine dam.

Although it was unlikely, an enemy landing on the territory of Dobrogea through the mouth of Sfântu-Gheorghe was taken into consideration. In this regard, for the swap of the troops, the road making the connection between Mahmudia

[10] *Ibid,* p. 916.
[11] *Ibid,* p. 917.
[12] *Ibid,* p. 919.

and Acaclău had to be protected and maintained. If the Russians were able to cross the Danube, the Romanian front being moved behind the river, the Romanian strategists considered that the main attack direction of the bulk of enemy troops would have been Babadag city, the old Turkish fortress-capital, while four batteries located on the heights around the city would have focused on the North road and Toprak-Kiopu bridge. However, the main objectives of Russians in Dobrogea would have been the two crossing points to the positions behind the line Focșani-Nămoloasa, namely Hârșova and Cernavodă[13].

ROMANIAN PLANS FOR THE DEFENCE OF THE DANUBE LINE BETWEEN OSTROV AND AZACLĂU POINTS

If the Russians had succeeded to force the line of Danube, after the fall of Babadag city, the enemy troops would have concentrated on Hârșova and Cernavodă, leaving Constanța city on the left flank. Due to the fact that the river makes a right turn in Brăila-Galați area, the left shore dominates the right shore. Moreover, because of the marshy terrain around Măcin, a passage of troops through this sector would have been very difficult. In the North, upstream, there is Hârșova fortress, an important passing point very used in the previous centuries. In order to prevent the arrival of the Russian fleet to support the ground troops which were already on Dobrogea land, it was proposed the positioning of a coastal battery on the hills around Brăila, as well as a torpedo dam at Azalcău.

The crossing point of the river there was recognised as favourable in both ways even since the wars in the 18th and 19th centuries, Marshal Helmut von Moltke the Elder appreciating, in this regard, that *Hârșova was a stable bridgehead against the Turks*[14].

In the 1806-1812 campaign, the Russians established at Vadul Oii, near Hârșova, a bridge at the end of which they built fortifications and other engineering works for defence. This fact attracted from the Turks the decision to strengthen the position of Hârșova fortress with separate works outside the wall that surrounded the fort. That's the reason why, the same great German strategist and military leader appreciated that Hârșova was a strong fortress *that could not resist against an attack from Dobrogea, here being able to oppose a vigorous resistance*[15].

[13] *Ibid,* p. 921.
[14] Marechal Helmut von Moltke, *Campagnes des Russes dans la Turquie d'Europe en 1828 et 1829*, Paris, 1854, I-er volume, p. 76.
[15] *Ibid*.

Taking into consideration the composition of the land, namely the branches of Ciobanu hill that descended towards the fortress, reaching to Băroiul brook at the height of 84 m, there was the possibility to build some similar, additional works, meant to increase the defense ability of the fort against an attack coming from East and South-East. The engineering works would have continued with the construction of a bridge on Vadul Oii or through Gâsca Mare islet to refuel the troops that formed the defensive system of Hârșova[16].

In these conditions, the position of Cernavodă would no longer be the object of the Romanian defensive in the case of an attack executed from North or East. Once Hârșova had fallen, the Focșani-Nămoloasa-Galați line, the main target of the Russian troops, would have been easy to reach.

MEASURES TAKEN BY THE ROMANIAN AUTHORITIES FOR THE DEFENCE OF THE MARITIME COAST

Colonel Marin Ionescu-Dobrogeanu also considered that, due to low bathymetric quota, the only ports that could be used by the warships would be Sulina and Constanța. But still, due to its position, but also to the lake that could have sheltered smaller boats, in the defense plans of the coast of the Romanian Navy could also have entered the position of Mangalia from the South of Dobrogea. But this was impossible, in the case of an attack executed from the sea by the Russian naval forces. Sulina, protected by the provisions of the European Commission of Danube, could have guaranteed the free passage of the Russian ships which, as recalled above, would hit the fortifications around Tulcea. In discussion remained the defense of Constanța city, which was an objective of first importance, both strategic and tactical one, on the Romanian coast of the Black Sea.

Following the works that were executed since the beginning of the 20th century, the capacities of the port basin being extended to approx. 1.5 km towards the sea, the vulnerability of the city and the port increased in front of an offshore attack. The general appreciations were that the city could not resist more than a few hours against of a powerful attack of a cruising and destroying fleet, a 2/3 of its perimeter being discovered. Thus, in order to increase the defence capacity, the author of the study proposed the building of a coast battery formed of heavy cannons located in the area of Carol hotel and Vii point, the city's higher promoters.

[16] Marin Ionescu-Dobrogeanu, *op. cit.,* p. 922.

It is worth mentioning that at this point of the discussion appears for the first, in fact, the only time, the proposal to build, after a Danish and French model, a defense line offshore, at more than 2,5 km from the coast, formed by a dam measuring 1,377 m, where the depth of the water would not be greater than 20 m, with a shape of a line broken at 140°, provided in the centre with a strong fort, flanked on the sides by two other secondary forts, to form a system with the mentioned coastal batteries[17]. Moreover, for the internal defence of the port, on the heights near the Military Hospital, according to the proposals of General Henri Alexis Brialmont[18], it would have been indicated to build a fort after the model of Spithead fortresses from the defensive of Portsmouth port or Constadt for Petersburg[19].

THE ROMANIAN DOCTRINE FOR THE DEFENCE OF DOBROGEA AGAINST AN ATTACK CARRIED OUT FROM THE SOUTH

In the first decades after Dobrogea returned to Romania, no serious study to debate the Romanian defense at the South border of the province between Danube and Black Sea was carried out[20]. This represented a lack in the Romanian defence system, all the more since the border line, the way it was traced, was very difficult to cross.

Among the main points where troops stationed, namely Arab-Tabia, Asarlâc, Cafalchioi and Mangalia, there were several tens of kilometres away, and the valleys crossed the border, and where pretty steep and abrupt, making the communication less efficient in case of a Bulgarian attack.

According to another study at the end of 19th century, signed by young Lieutenant Athanasie Napoleon, under the guidance of the military geographer, Lieutenant-Colonel Iannescu, namely *Dobrogea* și *Gurile Dunării*, published in Bucharest in 1896[21], even a second line of defence of the above-mentioned border *would have been pretty difficult*, stretching over more than 100 km, between Rasova-Cocargea-Cobadin-Musurat. Also, this crossed the Diordumgi-Orman valley and, according to Colonel Ionescu-Dobrogeanu, the execution of such a defence line would have been a serious strategic mistake, on the same above mentiond considerations. He also considered that the angle of the border in the Asarlâc point was not favourable to the Romanian defensive, the region included in the triangle Asarlâc-Cuzgun-Ostrov being redundant from this point of view.

[17] *Ibid*, pp. 922-923.
[18] General Henri Alexis Brialmont, *Progreses de la defences des etats*, Bruxelles, 1898, pp. 189-190.
[19] Marin Ionescu-Dobrogeanu, *op. cit.*, p. 923.
[20] *Ibid.*
[21] Locotenent Ath. Napoleon, *Dobrogea* şi *Gurile Dunării*, Bucuresci, Tipografiile *"I.V. Socecu",* 1896, pp. 69-70.

Of course, the direction of movement of the Bulgarian troops would not have been along this road for the same considerations.

Eliminating the hypothesis of a puerile tactical approach to attack the target[22] directly, and moreover leaving the right flank of the Bulgarian army uncovered, the best hypothesis to consider in this case would have been an enemy offensive from Hagi-Oglu-Bazargic direction, that crosses the border in the less rugged area, in the Bairamdede-Cobadin-Medgidia area, facilitating avant-garde actions on the right flank that also threatened the position of Constanța port.

In this case, the Romanian defense should have relied on the landforms. Taking also into account that the Bulgarians could have placed some detachments in the difficult zone of the western part of the province, namely at Asarlâc, the target to defend, respectively the position of Cernavodă, would have been threatened from two directions, coming from South and East. Therefore, the centre of the Romanian defense should not be positioned as close to the target as the Danube River. According to the Romanian author mentioned so far[23], this had to be in front of Carasu valley, benefiting from the natural obstacles represented by Urluia and Borungea valleys, somewhere in the Enigea area, from where the Romanian troops could counterattack towards South to Chioseler, to cope with the bulk of the Bulgarian troops that were moving forward to Bairamdede-Cobadin. The Cuzgun could easily be defended due to the heights in the area, the Southern detachments not posing a threat.

If this first defence line was lost, the new defensive system had the city of Medgidia on the Peştera-Ikingi-Dere alignment in the centre, from where it could extend to the sea, using the traces of the Roman earth wave, known as *Valul lui Traian (Traian's Wave)*, to Murfatlar city.

The Black Sea coast, between Balcic and Chilia Veche, was assigned to the Sea Division to which, in addition to its own forces, some units of the ground troops were also subordinated (rangers, sedentary parts of some regiments, gendarmes, territorial troops etc.)[24].

[22] It is about the position of Cernavodă, which, once conquered, would have allowed the insulation of Constanța and a large part of Dobrogea from Romania, as well as the advance of the enemy troops towards the capital.
[23] Marin Ionescu-Dobrogeanu, *op. cit.,* p. 924.
[24] On 26 February 1896, the *Law for the organisation of War Fleet* was approved, published in the *Official Gazette* no. 279 on 13 March 1896, according to which the Sea Division and the Danube Division, which were newly established great units, were subordinated to the War Fleet Command. In the initial composition of the Sea Division entered the Crew Depot with the School of Officers, the School of Torpedoes (Mobile Defence), the Defence of Maritime Ports, *"Elisabeta"* cruiser, the *"Mircea"* school-ship, *"Grivița"* gunboat, *"Sborul"* and *"Năluca"* torpedoes. See Anton Bejan (coord.), *Dicționar enciclopedic de marină*, Editura Societății Scriitorilor Militari, București, 2006, p. 173 and Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Tanța Mândilă, Ion Rîșnoveanu, Florin Stan, Andrei Vochițu, *Istoria Statului Major al Forțelor Navale. 1860-2010. Monografie,* Centrul Tehnic-Editorial al Armatei, București, p. 56.

In 1903, when, for the first time, a training march was carried out on Prut and then on the Danube, to Turnu Severin[25], one of the objectives was to seriously bring into discussion, followed by debates, war issues necessary for the coordination of ideological aspects and establishment of an official naval doctrine.

It is worth mentioning that the military theorists understood the historical character of the principles of a doctrine that *must be kept updated in order to be the true expression of current military science, because it is not a religious dogma, which is unchanged and must be applied ad-literam in all parts and always*[26].

ROMANIAN NAVAL DOCTRINE AT THE END OF THE 19TH AND THE BEGINNING OF THE 20TH CENTURIES

The ideal naval doctrinal framework was able to truly fall into place by a legal support[27]. Thus, starting with May 1879 until the end of the 19th century, *The Police Regulation of the Danube ports and shores of Romania, the Regulation of the personnel of the navigation and ports service, the Law for the organisation of the Fleet and the Service of ports,* with the *Special regulation* of this law, appeared. Also, as in any beginning, new related institutions were set up[28].

Nevertheless, General Constantin Hârjeu criticised, in 1907, the fact that the General Staff *could not build up an [official n.n.] doctrine, either in the form of regulations or in the form of instructional methods, nor to give a better orientation to the organisation of the army*[29].

Related to the maritime domain, in Romania, the term *doctrine* was perceived as a system of fundamental principles with which the naval forces carried out their missions[30]. In this context, the War Navy, generally, had to provide effective support for the protection and defence of territorial integrity. The doctrine was the one that determined the most efficient ways of practising the use of naval forces under the existing conditions[31].

[25] AMR, *2568* fund, file 345, *Memoriu rezumativ asupra pregătirii de război, ipotezelor de război,* şi *principiilor de doctrină* între *anii 1900-1916*, f. 139.
[26] *Revista infanteriei*, year XXX, March 1913, p. 275.
[27] Colonel G. Iannescu, *Studii de organizaţiune militară. Armata română. Ce a fost, ce este, ce ar putea să fie,* Bucureşti, 1906, pp. 416, 418; see *Istoria militară a poporului român,* vol. V, Bucureşti, Editura Militară, pp. 305-306.
[28] Dr. Carmen Atanasiu, *Problema suveranităţii României la Dunăre şi "Navigaţia Fluvială Română" (1919-1945),* Bucureşti, Executată la S.C. *"Nelmaco"* S.R.L., 2003, pp. 39-40.
[29] General C.N. Hârjeu, *Rostul cuvintelor: Disciplină, Doctrină, Iniţiativă*, Bucureşti, 1907, p. 162.
[30] Ion Ionescu, *Primele elemente* şi *principii ale doctrinei navale româneşti (1878-1916),* in *Anuarul Muzeului Marinei Române*, vol. VIII/2005, Editura Compania Naţională Administraţia Porturilor Maritime, Constanţa, 2005, p. 154.
[31] Traian Atanasiu (coord.), *Puterea maritimă şi diplomaţia navală,* Editura Militară, Bucureşti, 1998, p. 59.

Naturally, the naval doctrines should have appeared where there were expansionist interests, big fleets, diversity of ships and naval tradition, but the great Maritime Powers did not feel, in the pre-modern era, the need of excessive conceptual theorising, regarding their interests and the consolidation of defence capacity of national or economic spaces in the immediate vicinity or overseas territories, because they were acting discretely based on the law of force, not having to justify in front of any organism, much less off the planetary ocean.

The necessary regulations, when they appeared, were made by the great powers through conventions and treaties, more or less transparent in which, usually, the little ones were not even taken into consideration, without the chance to become a legal part, subject of law of those respective regulatory acts[32].

The need to find the best way of action for asserting interests on the water, as state reasons, by ordering ideas *according to time and circumstances for their smart employment*[33], was felt by the small countries, later named secondary naval powers, dependent on protectors and allies.

With the evolution of thinking, in general, and the evolution of legal thinking, in particular, law enforcement became a consequence of the new relations between the states.

Almost in parallel, the naval doctrines became closed systems of thinking and, as a consequence of education, especially the one practiced in the Higher War Schools, which became, in time, centres of development of science and doctrine, of spreading the general military culture[34] in an historical stage that coincided with the last three decades of the 19th century.

In Romania, as a result of the experience gained following the sharp Independence War, opinions, ideas and concepts appeared regarding the actions of fighting on the water.

Thus, the 1877-1878 moment really represented a turning point in the Romanian thinking, military and naval-wise, because:

- there was no longer any military or diplomatic tool to intervene in Romania's favour, by the disappearance of the suzerainty protective power, at least theoretically;
- independence required the creation of new entities and state political-military organisms with forces and specific means, the resizing of the existing ones and which, in their entirety, had to become functional and systemic;

[32] Ion Ionescu, *op. cit.*, p. 155.
[33] *România militară*, year XXX, March 1913, p. 275.
[34] Locotenent-colonel Ioan Popovici, *Organizarea armatei române,* Roman, 1900, pp. 116-119.

- the situation changed with the appearance of a coastline of approx. 240 km whose defence task fell, in the first place, in the responsibility of the Romanian naval forces;
- the access to the free sea created a new perspective and led, somehow, to rethinking the concept on the new maritime-fluvial dimension of Romania's defence.

Thus, concerns for the formation of naval doctrinal principles increased, with some positive results[35].

For starters, naturally, the main naval doctrinal idea proved to be insufficiently developed, here and there confusing, tending to simplistically adopt some foreign solutions. In time, the approach manner changed, the problem being treated and concluded gradually, adapted to meet the requirements of a Romanian conception demanded by the specific national needs of defence on the sea and river, facts that occurred, more significantly, starting with the last decade of the 19th century.

As a result of these realities, at governmental level, following the debates and pertinent analyses, imposed by the fundamental idea of keeping the hard-won statehood, the first naval modernisation program of the Navy appeared in 1881[36]. Then the first theoretical models were created, depending on the situations that had to be solved based on the diversity of conceptions, but also on the unity of views in their application[37], *so that all elements work in the same direction*[38], of coexistence with the war issues[39].

The insufficient number of ships necessary for the organisation of a military fleet, the inexistence of a commercial, maritime and fluvial fleet, the lack of long-distance navigation traditions, during 1860 and 1890, were essential impediments to the development of the maritime-fluvial component of the Romanian economy and, implicitly, the poor stimulation of the higher development of naval thinking.

[35] *Istoria gândirii militare* românești, Editura Militară, București, 1974, p. 193.

[36] Ion Ionescu, *Politica navală a României între anii 1919 şi 1941*, Editura Companiei Naţionale Administraţia Porturilor Maritime Constanţa, 2002, p. 64.

[37] Capitaine de vaisseau Gabriel Darrieus, *La guerre sur mer La doctrine*, Augustin Challamel Editeur, Paris, 1907, pp. 358-361.

[38] *Revista armatei*, year XIII, September 1895, p. 642.

[39] Ion Ionescu, *Primele elemente* şi *principii...*, p. 156. In this respect, the military decision-makers from Bucharest concluded that *Romania's Central European position, the fact that it obtain a Black Sea coastline exit only in 1878, the inability to become an economic, military or colonial power, the hesitant-selective politics for choosing the right moments to favourable allies are some of the causes that did not allow our country to gain the mentality of winner, but, history has shown that such attitudes have proven to be at hand solutions, compatible, as a rule, with the geopolitical situation, the structure of Romanian mentality, the type of country, demography and historical heritage.*

In these conditions, it is more difficult from the documents in the archive or from the specialised literature of the period 1878-1914 to establish a Romanian doctrinal navy framework because the action manner and the actions, by themselves, of Flotilla and, from 1898, of the Military navy, did not rely on an articulated, *ab initio*, specific and essential idea but, usually, on the needs demanded by the moment. In a careful analysis, only a few elements and relative principles, sometimes minimal, of Romanian naval doctrine can be exemplified[40].

Taking into consideration both the geographic configuration of the Western area[41] of the Black Sea, and the Danube River with its mouths and delta, these important water areas, in the conditions of an armed conflict, would have been transformed into theaters of operations, reason for which the actions of the Romanian naval forces against some presumed enemies or adversaries would naturally have been oriented towards East and South.

In the event of a war to the East, it would have been with the Russian Empire. Our flotilla should have played, equally, both the defensive and the offensive versions.

Compared to the potential adversary, it was inferior in forces and means and, in this case, Romania should have not focused on direct commitment, being put in the position to give up in extreme situations to defending the Gurile Dunării, its delta, the coast and the ports, forcing it to a passive defence under the protection of mine dams and coast batteries on the flank of the fortified line Focşani-Nămoloasa-Galaţi. In other words, the Romanian Navy could accept the commitment of its forces only in cooperation with the ground forces, in the subsidiary being able to observe that there was a tactical error by keeping, in reserve, the cruiser *"Elisabeta"*[42], considered the most powerful force, with the support of which to carry out the withdrawal of ships that were defending Cotul Pisicii[43], if they were rejected.

In this idea, from a tactical point of view, the use of a river flotilla, on the flank of ground forces, that would have relied on the Danube to prevent the return

[40] *Ibid*, p. 158.

[41] From Gura Musura to Vama Veche. After 1913, to Ecrene, the southernmost point of the Quadrilateral.

[42] The light cruiser *Elisabeta*, which bore, symbolically, according to the tradition of the time, the name of the sovereign of the country, was built in 1888 at *Armstrong* shipyards in Newcastle, entering the active service of the War Fleet on 15th of November of the same year. It had a displacement of 1,320 t, the length of 72 m, the width of 10.25 m and the total height of 6.68 m. The average speed of 18.1 Nd was provided by two machines with simple coal expansion with a maximum power of 4700 hp. The firepower of the ship was provided by six 150 mm Krupp cannons arranged sideways, four Nordenfeld guns with rapid fire, two Hotchkiss 37 mm cannons, two 11.43 mm machine guns and four 381 mm Whitehead bullet tubes. See also Anton Bejan (coord.), *op. cit.,* p. 195 and Ion Ionescu, Georgeta Borandă, Marian Moşneagu, *Noi contribuţii la istoria Marinei Militare române*, Editura Muntenia & Leda, Constanţa, 2001, p. 160.

[43] Strategic point, through its configuration; the place where the Danube passes from Muntenia to Dobrogea.

of this flank satisfied one of the first needs of such an army through the best use that could be granted to the Romanian Flotilla as a distinct naval force.

An easy cover should also be taken into account, towards the southern front, against a neighbour whose attitude was not specified, nor the possibility of intervention, on one front or the other, by the connection of an internal river line, because these meant nothing else but meeting an elementary strategic principle[44].

In the event of a war towards the south, with Bulgaria, the Military Navy, probably in the middle of the action of ground forces, operating against a weaker enemy, had to adopt a more offensive attitude. Therefore, strategists and tacticians claimed that, in practice, the principles and elements of the Romanian naval doctrine could be applied if it was considered as valid the fact that at the seaside, where with the help of *Elisabeta* cruiser and the two armed auxiliary cruisers, the lines of communication could have been under control, and at the Danube, where by distributing the groups of ships, on sectors, it was anticipated the crossing of the waterway and preventing the enemy to use it.

In applying this offensive principle, a tactical organisational error was made in placing a mine dam before the bridge of Cernavodă and the concentration of all means of defence of this main target it its immediate vicinity; it is easy to understand why the easiest variation in the game of forces could get the enemy close to the bridge, before the defender recovered or received help. The basic defence of the bridge had to be made at the border, and a defence against diversions was necessary around it.

Regarding the applicability of the naval problem of the time, from a critical point of view, it can be said that it was exaggerated in the appraisal of the means and it was not recognised that a river flotilla could not master (a term used in the mobilization works) the Danube when the enemy would have had under control one of the shores, and the groups of ships distributed on the sectors of the watercourse could only hamper the use of the waterway, without being allowed full control .

A great lesson resulted, namely that the divisions of ships on segments of responsibilities established the principle of Danube sectoral organisation, which proved to be very useful in the river war[45], a form which is still used even today.

At the beginning of the 20th century, great attention was given to the idea of resistance at the strategic point Cotul Pisicii, under the protection of dams

[44] A.M.R., *2568 Collection*, 345 file, *Memoriu rezumativ asupra programelor de război, ipotezelor de război* şi *principiilor de doctrină* între *anii 1900* -1916, p. 146.
[45] *Ibid,* p. 147.

and coastal batteries, in the possibility of abandoning the Delta's defence. Neither the establishment of a Danube fleet would not have brought any change in the naval doctrine, regarding the conduct of the war on the river in an armed conflict towards East, because the implementation of this idea would imply too much dependence upon the actions of land forces whose doctrine did not include Military Navy action, which could have been others, after the establishment of the Danube Squadron. It can be assumed that this state of affairs represented an asynchrony due to incomplete reasoning, by not studying the realities enough.

After the Second Balkan War, in 1913, our relations with the Russian Empire made a relative and short relaxation possible taking into account the interests of both states regarding the perspective policy of alliances. For this reason, the possibilities of a war with this neighbour were not studied anymore. If up to this date *Hypothesis A* represented the variant of a conflict with the East, in 1914, *Hypothesis A* referred to the south front, and no other hypothesis could be seen in the mobilisation preparations of the Military Navy.

Some other major conclusions could be drawn from the military action in 1913, which allow the coagulation of the naval doctrine regarding the conduct of hostilities on the water.

Thus, this war has proven the importance and necessity of increase of the number of commercial, transport ships, which greatly facilitated the mobilisation movements, the concentration of forces and the passage of the river. It also revealed the beneficial role regarding the usefulness of the flat boat bridges (of ships, as they were called at the time)[46].

In practice, as a general rule, it was clear that the flat boat bridges could only be built in the points where the land and naval forces owned the control of the river communication line, which involved, permanently, the mastering of both shores of that communication.

Thus, it was examined the possibility of building such bridges in points located in the Middle Danube, even if Romania had not controlled communication lines, up to those points. In such case, the materials necessary for the construction of communication bridges had to be concentrated, before the declaration of war, in districts close to these points, that had to meet certain safety conditions and which, in the same time, demanded the deployment of a part from Danube Squadron to guard the water, with all the inconveniences resulted from the fact that the squadron fraction remained unavailable for use on other battle fronts.

[46] *Ibid,* p. 167.

Also, it appeared as very necessary to build a special ship for the transport of cavalry and artillery, which were completely absent. Immediately after the Second Balkan War, this was an unresolved fact for multiple reasons.

It was considered mandatory to organise a position of resistance, on the river, with mined field, with coastal batteries and light artillery, in order to defend that field, with ships able to capitalise on the contribution of some extra-mobile batteries, torpedo preparation and launch stations and of the current mines, which could represent the most suitable defence when a flotilla or a lower river fleet had to resist against a similar, but higher, force.

The actions of the Austro-German fleet during the War of Integration, 1916-1918, confirm this principle and, if it tried to have an offensive attitude, no doubt it would have had so many losses[47] that a more solid balance would have been established between both naval forces.

The dynamics of a river fleet in offensive missions involved, in the first two decades of the 20th century, two phases: artillery actions in stationary (at anchor), rendered with barrage fires, through indirect firing over long distances and close actions executed with the moving ships, by using direct firings (direct shooting)[48].

There is the possibility of the enemy to use light ships to oppose the ships from defensive and the destruction of the mined field, a manoeuvre that would have resulted in big sacrifices from the attacker. This variant, however, required the existence of a fleet consisting of light ships that were prepared for this kind of attack.

It was insisted on the rapid adaptation of the human factor to the concrete situations in the theatre of operations, by moving from defensive to offensive. The coastal batteries fixed on the concrete sites, located on the shore that would have handled the troops of both belligerent parts, remained exposed to the human and material losses, either to the slightest changes of the front, which is why mobile artillery was chosen. Instead, the artillery on the opposite shore had the possibility of withdrawal, but also of firing until the last moment, and it was considered necessary to be installed in solid works, because the quota of the emplacement was low and uncovered.

It was accredited with the idea that a well-organised minefield, even if the land front had fallen, was capable of providing sufficient opportunities for ships and allied naval material to take relative shelter in this field.

[47] *Ibid,* p. 168.
[48] Ion Ionescu, *Primele elemente* şi *principii...*, p. 159.

Complementarily, the need for a remote information and surveillance service, by small patrol ships, without major military value and observation posts, on the friendly shore, was considered important and should never be neglected during the period of preparation and political tightening, prior to the war.

Isolated stations for the preparation and launching of torpedoes and current mines, which were not part of a defensive organisation, could be set up and used under conditions of non-discovery by the enemy, any other situation making them vulnerable.

It was envisaged that a river flotilla that would operate to the support of the flank of some ground forces should always be provided with a fleet of transport ships[49] to be able to board, but also to withdraw, the land troops which would eventually have been pushed to the Danube or would have been cut. From the practice of conducting the war on the water it was proven that an organisation of a bridgehead similar to that of Turtucaia, which was a disaster, had to have an easy bridge of pontoons for the safe withdrawal.

The installation of a mine dam on the Danube intended for a longer stay in the water was considered very difficult and, that is precisely why this problem remained unsolved, in the first place, for technical reasons[50]. The proposal of visible dams, with mines with reduced buoyancy, supported by floats, was not considered practical by most specialists for the simple reason that they were easily destroyed by remote shooting. More efficient was the combination of mines with negative buoyancy sustained with elements from the stockade. The most operative system was the installation of dams by mines, concurrently with the objective that had to be protected, provided the fast anchoring of each mine and the dismantling of the dam, without danger.

CONCLUSIONS

The period of neutrality, 21 July/3 August 1914-14/27 August 1916, prior to the participation in World War I, stimulated the preparation of the Romanian naval forces. This stage, for about two years, did not change the ideal naval doctrinal framework and led, at the same time, to the development of its content, constituting, for the most part, the foundation and reason of the principles of strategy and tactics that would have applied, no doubt.

It should be specified that the existence of naval doctrinal elements and principles, coagulated over decades, made it possible to deploy forces and means,

[49] AMR, 2568 *Collection*, file 345, p. 169.
[50] At the time, no type of mine, no matter how special, could remain active for a long time.

on the hypothesis (variant) of the enemy in the south, prepared for a long time, still in peacetime, through countless training exercises with troops. If there had not been a unitary conception, the strategic and tactical principles would have been hastily applied, demanded in a hurry and imposed by the current situations in the river operations theatre.

It can be appreciated that the Romanian naval forces, supplemented with various floating material, requisitioned from the state's commercial or private companies, had to act independently, with independent missions and actions, but complementary to the land forces, within the national defence system.

BIBLIOGRAPHY

Archives

1. Romanian Military Archives.
2. Romanian National Archives.

General papers

1. ***, *Istoria gândirii militare* româneşti, Editura Militară, Bucureşti, 1974.
2. ***, *Istoria militară a poporului român,* vol. V, Bucureşti, Editura Militară, 1988.

Specialised papers

1. Carmen Atanasiu, *Problema suveranităţii României la Dunăre şi "Navigaţia Fluvială Română" (1919-1945),* Bucureşti, S.C. "Nelmaco" S.R.L., 2003.
2. Traian Atanasiu (coord.), *Puterea maritimă şi diplomaţia navală,* Editura Militară, Bucureşti, 1998.
3. Anton Bejan (coord.), *Dicționar enciclopedic de marină*, Editura Societății Scriitorilor Militari, București, 2006.
4. Henri Alexis Brialmont, *Progreses de la defences des etats*, Bruxelles, 1898.
5. Gabriel Darrieus, *La guerre sur mer. La doctrine*, Augustin Challamel Editeur, Paris, 1907.
6. Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Tanța Mândilă, Ion Rîșnoveanu, Florin Stan, Andrei Vochițu, *Istoria Statului Major al Forțelor Navale. 1860-2010. Monografie*, Centrul Tehnic-Editorial al Armatei, București.
7. Constantin N. Hârjeu, *Rostul cuvintelor: Disciplină, Doctrină, Iniţiativă*, Bucureşti, 1907.
8. G. Iannescu, *Studii de organizaţiune militară. Armata română. Ce a fost, ce este, ce ar putea să fie,* Bucureşti, 1906.
9. Ion Ionescu, *Primele elemente* şi *principii ale doctrinei navale româneşti (1878-1916),* in *Anuarul Muzeului Marinei Române*, volume VIII/2005, Editura Compania Națională Administrația Porturilor Maritime, Constanţa, 2005.
10. Ion Ionescu, *Politica navală a României între anii 1919 şi 1941*, Editura Companiei Naţionale Administraţia Porturilor Maritime Constanţa, 2002.
11. Ion Ionescu, Georgeta Borandă, Marian Moşneagu, *Noi contribuţii la istoria Marinei Militare române*, Editura Muntenia & Leda, Constanţa, 2001.

12. Marin Ionescu Dobrogeanu, *Dobrogea* în *pragul veacului al XX-lea,* Atelierele Grafice *"I.V. Socecu"*, Bucureşti, 1904.
13. Helmut von Moltke, *Campagnes des Russes dans la Turquie d'Europe en 1828 et 1829*, Paris, 1854, I-er volume.
14. Ioan Munteanu, *Cadrilaterul – istoria unei controverse*, in *"Anuarul de studii de politică de apărare şi istorie militare. 1997"*, Editura Pro Transilvania, Bucureşti, 1997.
15. Athanasie Napoleon, *Dobrogea* şi *Gurile Dunării*, Bucuresci, Tipografiile *"I.V. Socecu"*, 1896.
16. Ioan Popovici, *Organizarea armatei române,* Roman, 1900.

Periodicals

1. *Revista Armatei*, year XII, October 1895, p. 782.
2. *Revista Infanteriei*, year XVIII, July-August 1914, p. 56.
3. *România Militară*, year XIII, December 1896, p. 355.

FOREIGN INTELLIGENCE COLLABORATION DURING KING CAROL II DICTATORSHIP (1938-1940)

Alin SPÂNU, PhD

Associated Teaching Staff, Faculty of History, University of Bucharest

In February 1938, King Carol II imposed his political will and turned from a mediator into an important actor. When the royal dictatorship was established, the political parties were banned, the military took over the leadership of counties and town halls and the structures of force were given increased powers. At the same time, Romania began to be isolated externally, because of both certain scenarios of the revisionist states and the conciliation policy adopted by England and France. Against this background, the Romanian intelligence services launched actions of exploration and information exchange with traditional partners (England and France), and with Germany, with multiple purposes. From the English and the French, help was needed to counter revisionism, while from the Germans we required cooperation regarding the Soviet space, all with the purpose of maintaining Romania's integrity. The results, not always favourable, were analysed and presented to political-military decision-makers, those who had to make the final decisions.

Keywords: Romania, Carol II, Special Intelligence Service, collaboration, USSR, Germany.

At the December 1937 elections, no party won 40% of the votes, so they could form a one-party government. Although it organised the elections, the National Liberal Party/PNL obtained 36%, followed by the National Peasant Party/PNȚ with 20% and the *"Everything for the Fatherland"* Party (the political group of the Legionary Movement) with 15%. On 28 December 1937, the King appointed Octavian Goga as Prime Minister, the leader of the Christian National Party, which ranked fourth in elections with 9.15% and dissolved the legislative bodies on 18 January 1938. At the same date, new parliamentary elections were announced, which were supposed to take place in early March 1938. The dissatisfaction of certain internal and external circles with the right-wing government programme, the intention of getting closer to Italy and Germany in terms of foreign policy and the electoral deal concluded by Octavian Goga with the Legionary Movement led to the King's decision to change the regime. It seems that the governments in London and Paris explicitly called for the removal of the Goga-Cuza cabinet and the appointment of a government meant to *"establish the dictatorship"*[1]. Therefore, on 10 February 1938, the King expressed to the Prime Minister the desire to establish a national union government and Octavian Goga resigned. On the same night, 10/11 February 1938, a government was formed under the presidency of Patriarch Miron Cristea. The first measures were the appointment of military prefects, decreeing the state of siege and censorship at national level[2] and the cancellation of the March 1938 elections, which ended the period of constitutional monarchy and opened the path towards the personal regime of King Carol II[3].

The new cabinet led by Patriarch Miron Cristea was *"an eclectic government"*[4], composed of centre-right people, animated by a spirit of duty and a touch of political opportunism, which had the mission to restore and maintain order in the country.

[1] Şerban Milcoveanu, *Vârf de lance. Secolul XX. Depoziţii de martor al epocii şi relatări de participant la evenimente*, INST, 2006, p. 217.

[2] For more details on the censorship measures of that time, see Ioan Lăcustă, *Cenzura veghează 1937 – 1939*, Editura Curtea Veche, Bucureşti, 2007.

[3] For more details on Romania's evolution in this period, see: Al. Gh. Savu, *Dictatura regală*, Editura Politică, Bucureşti, 1970. Florea Nedelcu, *Viaţa politică din România în preajma instaurării dictaturii regale*, Editura Dacia, Cluj-Napoca, 1973; Florea Nedelcu, *De la Restauraţie la dictatura regală. Din viaţa politică a României 1930-1938*, Editura Cartea Românească, Bucureşti, 1981; Ioan Scurtu, *Istoria României în anii 1918-1940. Evoluţia regimului politic de la democraţie la dictatură*, Editura Didactică şi Pedagogică, Bucureşti, 1996, p. 161-188.

[4] Ioan Scurtu, Gheorghe Buzatu, *Istoria românilor în secolul XX*, Editura Paideia, Bucureşti, 1999, p. 343.

That is why, the first measures taken were in this direction: the declaration of the state of siege, the establishment of censorship, the appointment of senior officers as prefects, a new law for the repression of offenses against public peace etc. On 20 February 1938, a new Constitution was drafted, four days later being submitted to public opinion *"for good science and purpose"*[5], and on 27 February 1938, it was promulgated. On this occasion, the new Prime Minister delivered a speech that was seen by contemporaries as *"a broad indictment for political parties"*[6]. The new Constitution revealed that the king became *"an active political factor"*[7], which exercised the legislative power through the National Representation (the deputies being elected for 6 years, and the senators for 9) and the executive power through the government. Nationally, the recrudescence of right-wing extremist actions increased, and the King shifted between harsh repression and attempts to bring the legionary movement closer[8].

From the administrative point of view, on 14 August 1938, a new law was promulgated, in which a new structure emerged – the Land, 10 in the whole country, governed by royal residents. On 12 October 1938, guilds of civil servants, craftsmen and workers were created (instead of the trade unions), and on 16 December 1938, the National Renaissance Front[9] was established, the only legally accepted party. On 22 June 1940, the Front of the National Renaissance was transformed into the Party of the Nation, a *"single and totalitarian party"*[10] and the same day the Law-Decree for the defence of the unique and totalitarian public order of the Romanian state came into force.

The third government led by Miron Cristea was formed on 1 February 1939, but the Patriarch was ill, which prevented him from taking the oath. In less than three weeks, on 21 February 1939, he went to France for medical treatment to improve his condition. The age, the medical conditions, the turmoil of the political life and, perhaps, the stress of the function contributed to his death, on 6 March 1939, at 23.35 hours, in the city of Cannes.

The new Prime Minister became Armand Călinescu, a former member of the PNȚ leadership, who switched sides to embrace the King's position in the action

[5] Ioan Scurtu, Gheorghe Buzatu, *op. cit.*, p. 344. The Constitution was published in *Monitorul Oficial* no. 48/27 February 1938.

[6] *Ibid*, p. 345.

[7] Ioan Scurtu, *Istoria României..., op. cit*., p. 162.

[8] For more details on the evolution of the Legionary Movement in that period, see: Ioan Scurtu (coord.), *Ideologie şi formaţiuni de dreapta în România*, vol. V (1938-1940), INST, Bucureşti, 2006.

[9] For more details on the organisation and functioning of the National Revival Party, see: Ioan Scurtu, Gheorghe Buzatu, *op. cit*., pp. 343-364; Petre Ţurlea, *Partidul unui rege: Frontul Renaşterii Naţionale*, Editura Enciclopedică, Bucureşti, 2006.

[10] Ioan Scurtu, *Istoria României..., op. cit*., p. 176.

of installing a strong-handed government. He had been Minister of the Interior and Deputy Prime Minister, so his appointment was not a surprise on the political scene. The only drawback was its anglophile policy, which was in opposition to European realities. The harsh measures against the legionary movement (or the Iron Guard) and the inflexibility in foreign policy culminated with his assassination on 21 September 1939 by a legionary band. For one week (21-28 September 1939) General Gheorghe Argeșanu was Prime Minister, in charge of leading the repression of the legionary movement, followed by Constantin Argetoianu, also very close to the King (28 September – 23 November 1939) and Gheorghe Tătărescu (24 November 1939 – 4 July 1940). The change of orientation in the foreign policy forced again the change of the Prime Minister, so that the position was entrusted to Ion Gigurtu, an industrialist known for his pro German views. This appointment could not save Romania from the territorial losses of the summer of 1940, so the King was forced to resort to one of the people who opposed him and who he had sent to the Bistrița monastery: General Ion Antonescu. On 4 September 1940, the General was appointed Prime Minister, the following day receiving *"full powers for the leadership of the Romanian state"*[11], which inaugurated the entry of Romania into a new political constellation.

King Carol II wanted power, he obtained it, but he did not rise to the level of rhetoric and times, despite all the attempted formulas of government. The dissolution of the constitutional political system, the sinuous path in the relations with the legionary movement and the lack of procurement of the Romanian armed forces can be blamed entirely on him. The interests of the Romanian state were the maintenance of territorial integrity, respectively the consolidation of national independence and sovereignty. In this respect, the state leadership had to identify the external threats and limit the internal vulnerabilities. After 10 years of rule, King Carol was unable to maintain territorial integrity nor to develop the capabilities of the Romanian state to the extent of being able to withstand external threats[12].

Between 1938 and 1940, revisionism reached its peak[13], and Romania was one of the victims of this policy initiated by Hungary and Germany. Externally, the rise of the revisionist political currents did not find strong opposition from France and England, which applied a conciliation policy. In March 1938, Austria was annexed to the Third Reich, without any opposition from the democratic states. A few months later, in September 1938, the Munich Conference (29-30 September

[11] The appointment and responsibilities of the Prime Minister were published in the *Official Gazette (Monitorul Official)* no. 205/5 September 1940, part I.

[12] For more details on this, see Mihail E. Ionescu, *Carol al II-lea şi securitatea naţională*, in *"Dosarele Istoriei"* nr. 5/2000, pp. 50-53.

[13] For more details on border changes at that time, see Aurică Simion, *Agresiunile naziste din Europa în anii 1938-1939*, Editura Eminescu, Bucureşti, 1983.

1938), attended by the Prime Ministers of Great Britain, France, Italy and Germany, decided to dismantle Czechoslovakia in the hope of maintaining peace in Europe. Anticipating the danger posed by Romania, King Carol II paid a visit to London[14] (15-18 November 1938) and Paris (19-21 November 1938) to receive the most effective political, economic and military support. On his return, he went to Berlin and discussed with Chancellor Adolf Hitler (24 November 1938) the evolution of bilateral and, in particular, economic relations. The latter were initiated at the level of specialists, on 12 February 1939 and were concluded on 23 February 1939[15], with the signing of an economic treaty. The much-needed Anglo-French support was achieved only by certain guarantees for territorial integrity, offered at the same time to Romania and Greece (13 April 1939).

The European political balance was broken by the conclusion of the treaty between Germany and the USSR (23 August 1939), known as the Ribbentrop-Molotov pact[16], by which the two states divided their spheres of influence between the Baltic and the Black Sea. The first transposition of the secret plan into practice was the attack against Poland on 1 September 1939, which resulted in an Anglo-French declaration of war issued to Berlin (3 September 1939), but without practical consequences. On 17 September 1939, Soviet troops entered Poland and, shortly, the two powers divided their areas of interest, according to the previously established details. Immediately after the attack on Poland, on 6 September 1939, the Crown Council proclaimed Romania's neutrality, and in the following period, the Romanian diplomacy tried to create a Neutral Bloc, to delimit the territorial aggressions and to create a defence system. Events on the continental political scene imposed a new economic agreement with Germany (4 April 1940) and an oil pact with Belgium, the Netherlands and France. Subsequently, the government discussed the reorientation of foreign policy to Germany, given its expansion on the continent and, in particular, the interest for Romanian petroleum products.

During the analysed period, the external intelligence collaboration was the responsibility of the Secret Intelligence Service (SSI), which took place at both the traditional, Anglo-French level and the German one, mainly through the exchange of data on the USSR. In 1938, the SSI notified the Abwehr about Soviet attempts to penetrate the 3rd Reich's intelligence services, providing actual intelligence in

[14] For more details on the position of the Great Britain regarding Romania, see: David Britton Funderburk, *Politica Marii Britanii față de România (1938-1940)*, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1983.

[15] For more details on this treaty, see A. Niri, *Istoricul unui tratat înrobitor (Tratatul economic româno-german din martie 1939)*, Editura Ştiinţifică, Bucureşti, 1965.

[16] For more details, see Emilian Bold, Ilie Seftiuc, *Pactul Ribbentrop – Molotov,* Institutul European, Iași, 1998; Alexandru Moşanu, Ion Buga (coord.), *Anexarea Basarabiei în anul 1940 de către Uniunea Sovietică – o consecinţă directă a pactului Molotov-Ribbentrop*, Chişinău, 2002; Ioan C. Popa, *Fața nevăzută a agresorului. Pactul Ribbentrop – Molotov și urmările lui pentru România,* Editura Semne, București, 2017.

this regard. Major Constantin Ionescu-Micandru, the head of the Eastern Front of the External Intelligence Section of the SSI, was sent to Berlin by his superior, Mihail Moruzov, in June and October-November 1939, on which occasions a connection system was developed and the contact persons of the two institutions were established. Between 22 and 24 June 1939, the Romanian intelligence officer proposed to the German party a *"concrete"*[17] collaboration for collecting data on the USSR. The German side replied affirmatively, mentioning that it did not have *"specialised elements"*[18] on this level, but it could contribute financially. Ionescu-Micandru declined financial support and initialled the bilateral agreement. During the second meeting, the Romanian major discussed with his counterpart, the head of the Eastern Front, Major Pruck, who wrote to him, on 30 October 1939, *"we have become friends with the devil"*[19], an allusion to the recent pact concluded between Berlin and Moscow, with negative and predictable consequences since then. The following day, the SSI representative was received by Admiral Wilhelm Canaris[20] and gave him *«The Analysis of the Romanian Armed Forces Intelligence Service for the Head of the German Armed Forces Intelligence Service»*[21], meant to strengthen the collaboration between the two institutions. The head of the Abwehr appointed Dr Wagner as the official representative in Bucharest, with duties on the oil area and counter espionage on the Danube. He was in the Romanian capital on 8-12 November 1939, on this occasion being received by the head of the SSI, Mihail Moruzov. Also, in November 1939, Major Pruck arrived in Bucharest and provided us with a list of identified Soviet agents active in Romania.

Some explosions in refineries and some train loaded with petroleum products crashes caught the attention of Abwehr, which saw them as acts of sabotage. As a result, on 10 December 1939, Admiral Canaris and Lieutenant-Colonel Bentivegni, the head of the Offensive Counterintelligence Section, came to Bucharest, where for two days developed the counter sabotage and counter espionage measures. Ionescu-Micandru went to the capital of Germany on 18 December 1939, and the

[17] Cristian Troncotă, *Mihail Moruzov şi Serviciul Secret de Informaţii al Armatei Române*, Editura INI, Bucureşti, 1996, p. 93.

[18] *Ibid*.

[19] *Ibid*, p. 95.

[20] Admiral Wilhelm Franz Canaris (1 January 1887, Aplerbeck – 9 May 1945, Flossenburg) a naval officer in World War I, in which he commanded a submarine and acted informationally in Spain. He continued his career after 1918 in the army intelligence service, and on 1 January 1935, he was appointed head of Abwehr, which he led until 1944. Following the attack on Hitler (20 July 1944), his involvement was proved, a fact for which he was investigated, arrested, tried and sentenced to death. For more details about his life and activity, in André Brissaud, *Canaris. Le «petit amiral» prince de l'espionnage allemand (1887-1945)*, Librairie Academique Perrin, Paris, 1970; Jaroslav Kokoška, *Amiralul Canaris* (translated by Teodora Alexandru-Dobriţoiu), Editura Militară, Bucureşti, 1970; Richard Bassett, *Spionul-șef al lui Hitler. Misterul Wilhelm Canaris*, Editura RAO, București, 2008.

[21] The document was edited in Cristian Troncotă, *Mihail Moruzov…*, *op. cit*., pp. 298-304.

topics of the talks were how to secure the Prahova Valley and the Danube.

At the beginning of March 1940, Mihail Moruzov went personally to Berlin, where he met his counterpart, Admiral Wilhelm Canaris, and General Wilhelm Keitel[22], the Chief of the General Staff. One of the practical applications of the bilateral talks was the strengthening of the security measures of the Danube ports. Captain von Weiss conducted an inspection in the port cities of Turnu-Severin and Orșova (22-24 March 1940) and found that the guard *"is not enough"*[23], the area of the oil tanks had to be strengthened and patrol vessels had to be equipped with rescue equipment.

The Abwehr liaison officer in Bucharest, Dr Wagner, met with Moruzov (3 May 1940) and asked how Romania would react in the event of a French-British attack in the oil area. Admiral Canaris returned to Bucharest (28-30 May 1940) and, on this occasion, an exchange of information about the Red Army took place.

The Germans correctly analysed Moruzov's intelligence power, as well as his influence on the King, so, in early September 1940, when King Carol II was forced to abdicate, they found a formula to oust the head of the SSI. He was invited to a trilateral conference, in Venice, exactly when the events that led to General Antonescu's call to power and abdication of King Carol II were taking place in Romania. Although he was offered a delay in returning to the country, Moruzov, perhaps too confident in his power and influence, chose to return. He was arrested, taken to the Capital Police Prefecture and then to the Jilava prison, where he was assassinated on 26/27 November 1940. The Chief of the Abwehr arrived on 7 September 1940 in Bucharest, and the next day he was received by the new Prime Minister, on which occasion the coordinates of intelligence collaboration were established. Admiral Canaris could have demanded both Moruzov's release and his silencing, especially after discovering actual data, in the archive of the French intelligence service, that he was working on more levels.

Collaboration with traditional allies was maintained through the exchange of information and reciprocal inquiries on continental geopolitical relations. For a fairer picture, Moruzov sent in a European tour Lieutenant-Colonel Gheorghe N. Petrescu, former military attaché in Rome, head of the 2 Counterintelligence Office of the 2nd Intelligence Section of the Great General Staff and assigned as tactical attaché with the SSI. During the period 3-18 March 1939, he visited Poland, Czechoslovakia,

[22] Fieldmarshal Wilhelm Keitel (22 September 1882, Helmsherode – 16 October 1946, Nuremberg) artillery officer, participated in World War I, led various departments in the Ministry of War (1935-1937) and the High Command of the Wehrmacht/OKW (1938-1945). On 8 May 1945, he signed the surrender of Germany before the United Nations, and the International Military Tribunal in Nuremberg judged and sentenced him to death (1946).

[23] Central Historical National Archives (ANIC), *Presidency of the Council of Ministries – Special Intelligence Service* Collection (PCM-SSI), file 22/1940, p. 50.

Germany, England and France, where he discussed with representatives of the intelligence services, but also with military and political factors[24]. A second tour took place only in France and England (27 March – 6 April 1939)[25], where he tried to find out about the way the political circles saw Romania and to purchase armaments. After his visit to Germany and a short break in Bucharest, Moruzov visited his counterparts in France and England, to test the possibilities of supporting Romania. The head of the Intelligence Office of the French General Staff acknowledged that he had a small staff and that the best intelligence he had on Germany was from the SSI. In London (31 March – 3 April 1940), Moruzov had the opportunity to see the disinterest and the coldness with which Romania was treated, both from a military point of view, by the refusal to export arms, but also economically, by the lack of interest regarding investments/acquisitions in/from Romania. However, according to Moruzov, the British proved to be *"much more realistic"*[26] than the French in analysing the geopolitical future of Europe.

Mihail Moruzov proved himself a player with strategic thinking, but the events outweighed the possibilities of action and reaction. He tried to use all means to obtain useful data for the country, possibly anticipating, played correctly in relation to his partners, but did not consider the possibility that they would make such a flagrant mistake against him. Perhaps too full of himself, he overcame his possibilities and neglected the preservation instinct, so he chose to return to the country at a totally unfavourable time for his career and, above all, his life. Ultimately, after 16 years at the helm of SSI, he did not imagine that those whom he protected during difficult times, led by Horia Sima, would choose the simplest option to silence him: his assassination.

BIBLIOGRAPHY

1. Central Historical National Archives.
2. Ioan Lăcustă, *Cenzura veghează 1937-1939*, Editura Curtea Veche, București, 2007.
3. Șerban Milcoveanu, *Vârf de lance. Secolul XX. Depoziții de martor al epocii și relatări de participant la evenimente*, INST, 2006.
4. Ioan Scurtu, Gheorghe Buzatu, *Istoria românilor în secolul XX*, Editura Paideia, București, 1999.
5. Cristian Troncotă, *Mihail Moruzov și Serviciul Secret de Informații al Armatei Române*, Editura INI, București, 1996.

[24] The report on the tour and the results obtained by Lieutenant-Colonel Gheorghe N. Petrescu was published in Cristian Troncotă, *Mihail Moruzov…*, *op. cit*., pp. 263-269.

[25] More details on the visits in the two countries in *Ibid*, p. 270-277.

[26] *Ibid*, p. 103.

THE SITUATION OF THE ARMY AT ROMANIA'S RE-ENTRY INTO WAR ON 28 OCTOBER/10 NOVEMBER 1918

Silviu-Daniel NICULAE
PhD Candidate, "Carol I" National Defence University, Bucharest

The situation of the Romanian army on the eve of the second mobilisation resulted from the carrying out of the demobilisation imposed by the Peace Treaty of Bucharest signed on 24 April/7 May 1918. In other words, when mobilisation was declared, the operational status of all the higher commands, general services and military establishments of the Romanian army was the one corresponding to the last budget drawn up in peacetime, that is, from 1916. All these commands, services and establishments depended on the Ministry of War, in terms of both management and administration.

Keywords: First World War, re-entry into war, the situation of the Romanian army, the second mobilisation, carrying out of mobilisation.

THE GENERAL SITUATION OF THE ROMANIAN ARMY IN OCTOBER 1918

In detail, this situation of the army at Romania's re-entry into war was as follows:

1) The order of battle. At the decreeing of the 2nd mobilisation, the Romanian army had all the superior commands, general services and military establishments, as *"they were provided in the last budget in peacetime"* (1916). All these commands, services and establishments depended on the Ministry of War, in terms of both management and administration. The large combat, tactical and strategic units of the army were 15 infantry divisions (1-15), grouped into 5 army corps (1-5) and 2 cavalry divisions (1-2). In addition to these large units, it also had special branches and troops, organised in special commands that depended directly on the Ministry of War, such as: heavy artillery, aeronautics, communication troops, border guards, gendarmes and naval forces[1].

2) Deployment. In the political and military situation in which Romania was at that time, when Muntenia, Oltenia and Dobrogea were still occupied by German-Austrian-Bulgarian troops, the whole army was deployed in the free territory of Moldova and in Basarabia. In Moldova, there were the commands, troops and services of the Army Corps 1 to 4. Army Corps 3 and 4 (only the part from Division 6 and Division 13) stayed in their normal peacetime deployment, and Army Corps 1, 2 and 3 (Division 5 and part of Division 6 and Division 13), whose usual peacetime deployment was in Muntenia and Oltenia, were temporary part of the units of Army Corps 4 and Army Corps 3. In Basarabia, there were the Army Corps 5 (Divisions 9, 10 and 15), which had the normal peace deployment in Dobrogea and in the eastern part of Muntenia, and Divisions 1 and 2 Cavalry[2].

3) Organic structure. The Army Corps consisted of: 3 Infantry Divisions and 1 Cavalry Brigade of 2 regiments. The organic structure of the divisions was different, from the point of view of the component infantry units, namely: Divisions 1-10 consisted of 2 infantry brigades, each brigade with 2 regiments (Regiments 1-40); in addition, each of these divisions had a battalion of mountain infantry (1-10 Mountain Infantry); Divisions 11-15 consisted of 4 infantry brigades, each brigade having 2 regiments (Regiments 41-80). The rest was the same for all

[1] Romanian Military Archives/Arhivele Militare Române (AMR), *Great General Staff* Collection, file 131, p. 90.
[2] *Ibid*, p. 91.

divisions, with 1 artillery brigade composed of 1 regiment field guns and 1 howitzer regiment; 1 battalion of engineers.

❖ *Infantry.* Regiments 1-40 each had 3 battalions. The battalion consisted of 4 infantry companies, of which 1 training and 3 personnel and 1 machine gun company (4 pieces); battalions of regiments from Divisions 9 and 10 were composed of the same number of companies, except that 3 infantry companies had the war strength, and the 4th company was of personnel. Regiments 41-80 consisted of a single battalion, with 3 infantry companies, with a small number of troops and a machine-gun company (4 pieces). The Mountain Infantry battalions were each made up of 4 rifle companies and one machine gun company (8 pieces)[3].

❖ *Artillery.* Field artillery regiments consisted of 3 divisions, each division having 3 batteries, of which 1 for training and 2 of personnel; a total of 9 batteries. The howitzer regiments consisted of 2 divisions, each division having 1 training battery and 1 personnel battery; in addition, a mortar trench battery; a total of 5 batteries. Artillery and howitzer regiments from Divisions 9 and 10 had the batteries with the war personnel. The mountain artillery regiments consisted of 2 divisions, each division having 2 personnel batteries and a training battery; a total of 6 batteries. The heavy artillery regiments consisted of 3 divisions, 2 of them having 3 batteries (1 training and 2 personnel), and the 3rd of 2 batteries (1 training and 1 personnel); a total of 8 batteries.

❖ *Cavalry. Cavalry Division.* Divisions 1 and 2 Cavalry consisted each of 3 brigades of 2 regiments, 6 regiments in total; in addition, 1 cavalry artillery division, 3 batteries each and 1 cyclists company. The Roșiori Regiments (1-11) and Călărași Regiment 3, which were part of the Divisions 1 and 2 Cavalry, consisted of 4 squadrons and one machine-gun group each, with 2/3 of the war strength. The Călărași Regiments and the Royal Escort Regiment, which were included in the organic structure of the Călărași brigades of the Army Corps, were each made up of 4 squadrons and 1 machine-gun group (4 pieces), apart from the Regiment 10 Călărași, which consisted of 2 divisions, both with reinforced strength and assigned to Divisions 9 and 10 in Basarabia[4].

❖ *Special troops.* The divisional engineer battalions were each made up of 3 engineers companies, 1 telegraph company, 1 bridge company and 1 warehouse company; Battalion 2 Engineers had, in addition, 1 warehouse of tools. The fortress engineers' battalion consisted of 3 engineers companies, 2 staff companies and 1 warehouse company. The railway regiment consisted of 8 railway companies

[3] *Ibid*, p. 92.
[4] *Ibid*, p. 93.

and 1 warehouse company. The pontoon regiment consisted of 2 battalions and a warehouse company. The river battalion had 2 training companies and 2 staff ones, and the river battalion had 3 training and 2 staff companies. The Specialty Battalion consisted of: 1 wireless telephone company, 1 projecting company, 1 technical company and 1 warehouse company. The car traction corps had: 1 company car drivers; 1 company driving trucks; 2 technical companies; 1 group of armored light trucks; 1 motorcycle company; 1 warehouse company; 1 warehouse of materials and gasoline.

❖ *Aeronautics.* a) The aviation corps had: 1 command; 1 deposit company; 3 aviation groups (1, 2, 3); 1 group training – schools (4); general aviation reserve (workshops and central warehouse). The aviation group consisted of 4 squadrons (2 reconnaissance; 1 fighter; 1 technique), each with 8 aircraft; in total 24 aircraft (except the technical squadron). b) The air station corps had 25 balloons[5].

❖ *Border guards.* The Border Corps had 3 regiments (1, 2, 3). The Border Guards Regiment consisted of 3 guard battalions (Regiment 3 Border Guards had only 2 battalions) and 1 training battalion.

❖ *Rural gendarmes.* The corps of rural gendarmes consisted of 3 brigades of 2 regiments each. The regiments structure varied between 4 companies (Regiment 5) and 11 companies (Regiment 2). The pedestrian gendarmes. The pedestrian gendarmes battalion consisted of 2 companies (1 in Iaşi and another in Bucharest) and 1 warehouse section.

❖ *The military navy* had: the Navy Command; the Danube Division; Sea Division; general warehouses; Navy Arsenal. The Danube Division had the monitors: *"Alexandru Lahovary"*, *"Mihail Kogălniceanu"*, *"I.C. Brătianu"* and *"Lascăr Catargiu"*. The Sea Division had only the *"Elisabeta"* cruiser.

4. The strength. At the demobilisation of the army, according to the Peace Treaty in Bucharest (art. 4), Divisions 9 and 10 Infantry and Divisions 1 and 2 Cavalry, which were in Basarabia, had the strength reinforced (2/3 of the war personnel), and Divisions 1-8 had the reduced peacetime strength; finally, Divisions 11-15 had an even smaller number, which represented only 1/3 of the number of Divisions 1-8, because the regiments of these divisions had only one battalion. From this situation, which is not different from the one the Romanian army had around the 2nd mobilisation, it follows that:

a. the total actual number of the Romanian army was 163,240 people;
b. the combat strength of the whole army was: 180 battalions; 260 batteries; 98 squares[6].

[5] *Ibid*, p. 94.
[6] *Ibid*, p. 95.

5. The state of army preparation for war

❖ *Training.* The number of troops was very small, due to the numerous assignments and deployments required by the guarding of depots of all kinds, agricultural works, cultivation of vegetable gardens, gathering of forages, a large number of animals in care, because of the demobilisation of the army. Thus, troops training was almost entirely suspended, except for specialists training, which was also quite diminished. The officers' training was also reduced; however, the army sought to complete the training of officers that returned from captivity. Normal training in the troop corps was planned to start on 1 November 1918, when agricultural works were completed.

❖ *Armament and ammunition.* According to the Focșani convention, from 1 March 1918, the artillery material of Divisions 11, 12, 13 was passed into the occupied territory; and in keeping with the Bucharest Treaty (art. 5) we were forced to send into the occupied territory *"guns, machine guns, handguns, ammunition depots and carriages",* which became available through the elimination of the units and the personnel stipulated in the same treaty. With all these difficulties, the General Staff made all the efforts and managed to provide the necessary weapons and ammunition for possible mobilisation. Thus, the commission set up at the General Staff to plan the armament and ammunition to be sent into the occupied territory, according to Art. 5 of the Bucharest Treaty and the convention concluded in Bucharest, on 15/ 28 August 1918, managed to send there weapons, machine guns, rifles and firearms that were old and not in service. Under these conditions, on the eve of the 2nd mobilisation, the Romanian army had a sufficient amount of armament and ammunition remaining in the free territory of Moldova, namely: 160 field batteries (75 Md. 1904, 75 French and 76.2 Russian) and 65 howitzers (105-150 gauge). This number of batteries was able to meet the needs of 18 divisions, considering the normal artillery supply of a division, 9 field cannon batteries and 3-4 howitzer batteries; 31 heavy batteries (120, 150 and 155 guns and 120 howitzers); 100 trench mortars of 58 m/m; 15 mountain batteries; machine guns (max. 6.5, St. Etienne and Hotsckiss of 8 m/m, English of 7.7 and Russian of 7.62), machine guns (Gladiator of 8 m/m and English of 7.7) and handguns were also sufficient for arming 18 divisions, with an average supply of 8 machine guns for a battalion and 6 machine guns for a company[7].

The remaining ammunition in Moldova ensured: 7-10 days of fire, for weapons and machine guns; 4-7 days of fire, for machine guns; 5 1/2 days of fire for grenades; 9 days of fire, for field cannon; 10-14 days of fire, for field howitzers; 5-15 days of fire, for heavy artillery.

[7] *Ibid*, p. 96.

The quantity of available ammunition, although sufficient for beginning possible operations, nevertheless limited the duration of the probable operations, because we had neither the means nor the facilities necessary for their manufacture in the country, nor the possibility to obtain them from the allies, from whom we were completely isolated at that time. However, on the other hand, Romania, given the situation it was in, could mobilise only a maximum of 10 divisions. It followed that the Romanian army had sufficient armament and an average ammunition quantity of 15-20 days of fire, which fully justified the renewal of arms in these circumstances[8].

❖ *Subsistences and equipment.* The economic state in which Moldova was after the Peace Treaty from Bucharest was signed created a very difficult situation in terms of meeting the food and clothing needs of the army. Industrial facilities were quite reduced and their production capacity was limited; and the resources of the territory were drained by the war and the overpopulation of Moldova. The Ministry of War and its supply bodies were not able to make available the equipment and subsistence necessary for the army that was under arms, to create deposits and reserves for mobilisation, because in this situation the supply of the army and the civilian population was made by the Ministry of Industry and the Supply Department, established at the Presidency of the Council of Ministers. The need to ensure the existence of the civilian population meant that part of the War Ministry's subsistence deposits, as well as part of the army's reserve feed, was passed on to the Supply Department, which distributed them to the civilian population. Under these circumstances, even the troops under arms were deprived of food and clothing[9].

Subsistence. The quantities of subsistence found on the troops and in the warehouses of the Ministry of War were far from the supply needs of the army, in case of any mobilisation. In the country, however, there were supplies that could feed the army for at least a month; and their gathering in warehouses required 10-15 days.

❖ *Equipment.* The equipment available was quite insufficient, compared to the planned staff to mobilize (200,000 people). Among the main items were missing: 50% coats, 60% jackets, 40% pants, 15% boots (existing footwear was degraded), 10% shirts, 25% drawers.

❖ *The sanitary and pharmaceutical service.* Since the demobilisation of the army, most of the troops remained without doctors, because of the 149 corps troops, only 77 had military doctors, and the rest used civilian doctors. The inferior

[8] *Ibid*, p. 97.
[9] *Ibid*, p. 98.

sanitary personnel were also insufficient for the peace strenght, because during the campaign the people from the last 2 contingents, necessary for the health specialty, had not been assigned to the sanitary companies. The sanitary formations of the campaign had been completely abolished, with the demobilisation of the army, according to the Peace Treaty in Bucharest. The sanitary material had been collected from the troops, which had no place to keep it; but the classification of this material had not yet ended at the date of the 2nd mobilisation and because of this the endowment with sanitary material of the different formations encountered difficulties. The amount of existing sanitary material was plentiful, although part of the campaign sanitary material had been sent at different peace formations (hospitals, sanitariums). Part of the sanitary material such as: bags, tents, trolleys, canvas, towels, stoves was in the same state of degradation in which it remained at the demobilisation, their repair could not be carried out due to lack of funds, material and workshops[10].

❖ *Veterinary service.* At the demobilisation of the army, besides the active military veterinary doctors, there were still a number of 70 reserve veterinarians, temporarily called into service, so at the 2nd mobilisation, the army still needed a number of 40 veterinarians. The training of horse nurses and horsemen was completed by the special school, which worked after the demobilisation of the army. Surgical and horsemanship material, as well as the vaccine required for mobilisation, were also completed.

❖ *Horse Service.* The number of army horses was very small because, besides the number of horses sent in Muntenia with the artillery equipment, the command of the German Army of Occupation forced us to sell another 3,557 horses, the best ones. Filling the number by import from Argentina could not be achieved until the second mobilisation. At this time, the infantry regiments, the howitzer and heavy artillery regiments had a number of horses that outweighed the budgetary effective; the field artillery and the cavalry regiments (they had about 100 horses by squadron) had also deficits in horses compared to the budgetary effective. In Moldova and Basarabia, however, there were the necessary means for completing the mobilisation effective of units and services belonging to the mobilisable divisions of Army Corps 3, 4 and 5. At the demobilisation of the army, a large number of horses remained, but they were extremely weak, due to the shortages in the winter of 1917/1918. For their care, the troop had neither people nor feed. The scab that had become chronic and their terrible physiological state

[10] *Ibid*, p. 99.

had made them unusable. In order to be saved, they had been distributed free to the inhabitants, keeping only the strictly necessary ones at the units. But due to the lack of food in the summer of 1918 and because of the poor condition they were in at that time, many of the horses died and others were slaughtered at the slaughterhouse. So, in general, there was a lack of horses[11].

❖ *Communications.* When the army was demobilised, the entire telegraph-postal service was passed to the General Post, Telegraph and Telephone Department and the personnel and material had been evacuated to Bucharest, under German occupation, without the knowledge and advice of the General Staff. Direct telegraphic and telephone connections between General Staff and commands, the military telegraph-telephone offices from Iași, Vaslui, Bârlad, Tecuci, Galaţi, Bacău and Botoșani, as well as those of the Basarabia commandments had been abolished by the government. The wireless telephone service that had 4 goniometric positions (Iaşi, Chișinău, Bolgrad and Bălţi) had also passed in September to the General Post, Telegraph and Telephone Department so that the specialities battalion remained without staff and personnel and unable to train new staff. There were also 4 pigeon stations, in Botoșani, Chișinau, Bălţi and Bolgrad. Therefore, the measures taken by the government and the General Post Department to carry out the terms of the Bucharest Peace Treaty paralysed all the measures taken by the General Staff for the purpose of preparing the communications for war. For this reason, at the mobilisation, establishing and manning military offices were a difficult task, due to the lack of personnel, which had been evacuated to Bucharest; the repair of the lines destroyed by the German troops in retreat and the inclement weather was incomplete, due to the lack of material, which had also been evacuated to București[12].

❖ *Transport.* At the time mobilisation was declared, there were 817 locomotives in Moldova, of which only 163 were operational and about 14,000 wagons. Due to the small number of locomotives in operation, the possibilities for rail transport were rather limited. Repair of the damaged material could not be performed due to lack of raw materials, workshops and spare parts. The fuel situation was also precarious. The fuel reserve, proposed by the General Staff, which had allocated for this purpose 4 battalions of workers, for the cutting of wood in different forests, had not been fully achieved, because although in the forests there were 90,000 m.c. (4,500 wagons) cut wood, the transport to the stations was not organised and the crisis persisted. In October 1918, the General Department

[11] *Ibid*, p. 100.
[12] *Ibid*, p. 101.

of Railways obtained from the German Occupation Command 90 wagons of fuel daily, brought from the occupied territory. Under these conditions, at that time, the fuel supplies were only for 5-6 days and only for 8-9 liners daily.

THE CARRYING OUT OF MOBILISATION

1) The measures taken for the army to enter the war

The High Decree regarding the mobilisation of the army was given by King Ferdinand on 27 October 1918 in Iași and stated: *"Art. I. All the commands, army corps and services of the army are at war. The first day of mobilisation: 28 October 1918. Art. II. The war troops will be supplemented with people from the reinforcement, reserve and militias contingents, up to the 1894 contingent included"*.

In order to implement the High Decree, the General Staff gave the same order to all commands that the mobilisation would be executed according to the instructions given by the General Staff in July 1918. However, the rush with which the mobilisation had to be carried out, in order to help the Danube allied army in the operations of the Danube crossing, as well as the technical difficulties, caused the mobilisation directives to be changed even from the beginning. Thus, on the very first day of mobilisation – 28 October 1918 – the General Staff changed the first stipulations of these instructions, stipulating in the order that it stated that *"the people from reinforcement contingents will be called, i.e. the 1916-1912 contingent included, from Moldova. For the call of the reserve and militias contingents, orders will follow".*

Regarding the call of the reserve officers, the General Staff also decided on 28 October 1918 that *"out of the inferior reserve officers only the youngest second lieutenants and lieutenants will be kept mobilised, needed to man the staff resulting from the table with personnel under arms and contingents 1916-1912"*[13].

Also on the first day of mobilisation, the General Headquarters specified the number of units to be mobilised and the number of personnel as follows: a) No longer mobilising: army headquartiers; heavy artillery divisions; the units in group II[14]. Therefore, the following structures were to mobilise: Divisions 6, 7, 8, 9,

[13] *Ibid*, p. 102.

[14] The instructions given by the General Staff on 1 July regarding the mobilisation of the army stipulated that it would be done in 2 large groups: Group I, comprising units and services, which given their normal deployment would mobilise in a relatively short time, namely: Divisions 6, 7, 8, 13, 14, which had the majority of reservists in Moldova; Divisions 9, 10 and 12 Cavalry, which were in Basarabia and had reinforced effectives; Divisions 1, 2 Mountain Infantry and Border Guards, which consisted of mountain infantry battalions (which actually had larger numbers than the infantry regiments) and border guards regiments (which almost had the mobilisation strength). Group II comprised the rest of the large units, army corps and services that were part of the army, whose reservists were in the occupied territory.

10, 13, 14, 1 mountain infantry and 2 mountain infantry; 1 cavalry and 2 cavalry; army corps commands; mountain divisions; the air defence division; wireless telegraph stations; aeronautical groups; pontoon companies; sections of cars, ambulances, trucks; detachments of pedestrians and rural gendarmes. The border guard regiments were mobilised but without the establishment of the Border Division[15].

b) The strenght

I. Troops. The infantry had to mobilise the contingents 1912-1916 and only for the infantry and mountain infantry regiments, which entered in the structure of the divisions mentioned above. For infantry companies, the number of 100-120 people was established and for the machine-gun companies the number of 126 people. Company 4 from the battalion was dissolved, with its staff being completed the other companies in the battalion. The marching units were no longer organised.

The cavalry mobilised the regiments of cavalry and Regiment 3 Cavalry which entered in the structure of the 2 cavalry divisions, as well as a squadron of the regiments: 1, 2, 4, 5, 6, 7, 8, 9 and 10 Cavalry, intended to form the divisional cavalry of the mobilised divisions. For both the cavalry divisions and the divisional cavalry, the number of about 100 people was fixed for a squadron. In order to complete the numbers, the 1915 and 1914 contingents were mobilised[16].

Artillery. The artillery and howitzer regiments of the mobilised divisions called the 1908-1915 included contingents. The battery was still with 4 guns and 6 caissons. Mountain artillery and air defence mobilised the same contingents.

Pioneer troops and communications. Battalions 6, 7, 8, 13 and 14 Engineers each mobilised: a company of engineers, a section of light bridges and 2 sections of telegraphy. Battalion 9 and 10 Engineers mobilised: one engineer company, one section of light bridges and one telegraph section. For the engineers and communications troops, the contingents 1915-1912 included were mobilised.

The aeronautics had to mobilise the 1915-1914 contingents and the rural gendarmes were to mobilise the 1912-1915 contingents.

II. Services

a) Ammunition columns

Each division mobilised a single column of ammunition, consisting of 3 semi-columns, one of them artillery, the second howitzer and the third infantry. The ammunition columns of Divisions 1 and 2 Mountain Infantry were mobilised by the artillery and howitzer regiments of Divisions 8 and 7 respectively. The people

[15] AMR, *Great General Staff* Collection, file 131, p. 103.

[16] *Ibid*, p. 104.

needed for the ammunition columns of Divisions 9 and 10 are given by the artillery and howitzer regiments of Divisions 8 and respectively 13.

b) Divisional ambulances

For each division, an ambulance unit was mobilised with a stretcher unit. The ambulance sections of Divisions 1 and 2 Mountain Infantry were mobilised by the Company 4 Sanitary. For the divisional ambulance units, the 1912-1915 contingents included were mobilised.

c) The divisional subsistence columns were each made up of: 1 column staff; 2 subsistence sections, mobilised by the train division of the Army Corps; 1 operating group, with cattle herd, formed by the care of the subsistence companies of the army corps. To complete the subsistence columns, the Divisions 3, 4 and 5 Train mobilised the people from 1912-1915 included contingets.

d) The divisional campaign bakeries were organised as follows: 1 staff bakery; 5 sections each with 2 ovens. To complete the effective, the subsistence companies 3, 4 and 5 mobilise people from the 1915-1912 included contingent.

Sedentary parties

Each mobilised troop corps must also form a sedentary part, consisting of the company (in the infantry), the squadron (in the cavalry) and the section (in the artillery) of storage. The commander of the warehouse unit was also the commander of the sedentary part. The rest of the people, left from the active parts, over the effective established above, were to be used for the guarding of the various deposits and the management of the army corps. For the organisation of the sedentary parts commands, an order was to be given later[17].

Horses. Meeting the needs of horses in units and services had to be done as follows: from the horses owned by the units, being kept by the inhabitants, only 2/3 of the number of those in a village, namely the best horses, had to be brought to the army corps; the remaining 1/3 were left in the preservation of the inhabitants. For the artillery regiments in the Bacău and Roman garrison, no more than 2,000 horses were brought from Basarabia, which had been provided in the instructions given for completing the necessary horses for the units in Group I. On 2/15 November, the General Staff, considering that, in this situation, the mobilised divisions no longer needed the complete divisional services, decided the following: 1) Ammunition columns were no longer organised. The divisions would therefore have available only the ammunition on the army corps and consequently the people belonging to these formations were discharged. 2) The ambulance

[17] *Ibid*, p. 105.

sections no longer used the carriages and vans. They would only have the necessary personnel for hospitalisation and 2 sanitary trucks. The number of an ambulance unit organised on this basis was: 8 officers, 97 troops, 8 animals and 4 vehicles. 3) The subsistence columns were no longer organised but instead a division of 2-5 trucks was available for each division. 4) The campaign bakery mobilised only 6 ovens. The subsistence company provided the specialised personnel (bakers) and the respective train division provided the conductors. The train division also made available to each of the campaign bakeries 50 waggons full of horses or oxen. The number of campaign bakers was: 2 officers, 149 troops, 243 animals and 64 waggons[18].

Mobilised units

From the total number of 15 infantry divisions and 2 cavalry divisions available to the Romanian army in peacetime, Romania could mobilise only: 5 divisions (6, 7, 8, 13 and 14) that were deployed in peacetime in the free territory of Moldova; 2 divisions (9 and 10) which, although had their peacetime deployment in the occupied territory, nevertheless had reinforced troops, at the date of the mobilisation decree; 2 divisions of mountain infantry that were established at the mobilisation; 2 cavalry divisions. That is, a total of 9 infantry divisions and 2 cavalry divisions were mobilised, making more than half of the entire army's staff. Out of these large mobilised units, 2 infantry divisions (9 and 10) and the 2 cavalry divisions were located and immobilised in Basarabia, due to the political and military situation of this Romanian territory, therefore they were not available for operations in Transilvania or in the occupied territory. Also, Division 8, which operated in Bucovina. Therefore, only 6 infantry divisions (6, 7, 13, 14, 1 Mountain Infantry and 2 Mountain Infantry) were available for western operations[19].

3) The way the mobilisation was carried out. The mobilisation of the large units proceeded as follows: the mobilisation of Division 6 was made with some difficulties and was delayed due to the fact that at the decreeing of mobilization a part of the territory of this division, namely the one corresponding to the units with headquarters in Focșani, was occupied by the German troops. The delay was also caused by the fact that, at that time, all the units of Division 6, with the planned staff, were ordered to enter the occupied territory to ensure the order and to take control of the deposits left by the enemy. Operations to complete the established mobilisation personnel continued until the beginning of December 1918, when Division 6 received an order to be transported to Transilvania[20].

[18] *Ibid*, p. 106.
[19] *Ibid*, p. 107.
[20] *Ibid*, p. 108.

Division 7, having all the elements for mobilisation in the free territory, was able to mobilise in good conditions. With all the bad weather, the people responded to the call, so that at the dates prescribed by the mobilisation instructions, the troops and services of this division, except for the artillery, were ready to be formed, with the full number of people, horses and vehicles. However, due to the lack of horses, the artillery could not mobilise all the determined units, so that not all the batteries could be ready by the time when the division started operations in Transilvania. The division could mobilise, in the beginning, only 2 batteries from Regiment 4 Artillery, and the rest was completed later. With regard to artillery, Division 7 encountered the same difficulty as Division 6.

When the mobilisation was declared, the situation of the units of Division 8 was as follows: Regiments 13 and 25 Infantry were in the garrisons of residence; Regiments 29 and 37 Infantry were in Bucovina, on the march to Cernăuţi. Regiment 12 Artillery and 17 Howitzers, each had a battery in Bucovina, organised by the entire available staff of the regiment, and the rest remained in the garrisons of residence, due to the lack of horses and harnesses. The army corps had in the garrisons of residence the assistant of the chief of staff with small personnel, which was insufficient to prepare and complete the mobilisation works. The command of the division was in the process of moving from Burdujeni to Cernăuţi, far from the mobilisation residences of the subordinate units, which had to communicate their mobilisation orders and instructions and at the same time involved in the management of the operations in Bucovina. For these reasons, the mobilisation of Division 8 was made under difficult conditions[21].

At the decreeing of mobilisation, divisions 9 and 10 were located in Basarabia and occupied sectors on the Nistru River. They had reinforced troops, approximately 10,000 people each division, effective that satisfy the actual conditions set for the 2nd mobilisation.

The mobilisation of Division 13 and 14 could not be effectively executed because they had the majority of the mobilisation personnel in the contingents in the reserve element, so that the completion of the personnel became impossible only from the complementary contingents determined to be called. In addition to the insufficient number of troops, the following obstacles were added to mobilise these divisions: Division 13 had in the occupied territory 1/2 of the infantry regiments (Regiment 47/72 and Regiment 48/49) and the artillery regiments (23 Artillery and 28/3 Howitzers); the units of Division 14 had to organise and satisfy all the guard services of the penitentiaries throughout the territory of the Army Corps 4.

[21] *Ibid*, p. 109.

Regarding the military and political situation, created by the conclusion of the general armistice, in day 4 of mobilisation, the General Staff decided that the regiments of these divisions that were to meet on the 8th day of mobilisation, remain in place in their garrisons and continue mobilisation. In fact, however, these divisions not taking part in the operations were no longer mobilised[22].

Division 1 and 2 Mountain Infantry

These divisions were created at mobilisation, by transforming the Mountain Infantry battalions which entered in the organic composition of the infantry divisions at peace into regiments and grouping these regiments into the divisions of mountain infantry as follows: Division 1 Mountain Infantry consists of Regiment 1, 5, 4 and 6 Mountain Infantry, coming from the transformation of the battalions of mountain infantry with the same number, which belonged to Divisions 1, 2, 7 and 4 respectively; Division 2 Mountain Infantry consists of Regiments 2, 3, 9 and 10 Mountain Infantry, which came from the transformation of the battalions of mountain infantry with the same number, which belonged to Divisions 3, 5, 9 and 10 respectively. The completion of the mobilisation forces planned for the regiments of the mountain infantry divisions is made from the resources and with the help of the infantry divisions to which the respective battalions of mountain infantry had belonged organically. This procedure was determined, on the one hand, by the situation of the territory of the country largely occupied by the enemy troops, and on the other hand by the rush with which the mobilisation was to be carried out. The artillery of the hunting divisions was formed by putting together elements from the existing infantry divisions, namely: The Division 1 Mountain Infantry, which was the first to enter Transilvania, had only 1 battery from Regiment 11 Artillery.; and during the operations in Transilvania it was assigned a battery from Regiment 12 Artillery, Regiment 17 Howitzers and Regiment 1 Mountain Artillery; Division 2 Mountain Infantry, which later entered Transylvania, initially had 1 battery from Regiment 4 Artillery, Regiment 24 Artillery, Regiment 8 Howitzers and Regiment 2 Mountain Artillery[23].

At the mobilisation, the Divisions 1 and 2 Cavalry were located in Basarabia and had reinforced troops, approximately 3,000 people for each division. The completion of the number of people was difficult because some of the demobilised people were in the occupied territory, especially those of the Division 2 Cavalry. But the greatest difficulties came from the lack of horses and their state of weakness, which made them largely unusable.

[22] *Ibid*, p. 110.
[23] *Ibid*, p. 111.

4) Difficulties and weaknesses encountered

The duration of the mobilisation far exceeded the time prescribed by the mobilisation instructions, both because of the weather, since winter had already begun, the transport difficulties, but mainly because of the lack of materials. In particular, they lacked the equipment, the means for subsistence as well as the horses necessary for artillery and cavalry. The lack of horses was so great that the divisions could not meet their needs regarding horses, at the beginning of the mobilisation, except for only one or at most 2 batteries of each artillery or howitzer regiment. Regarding the transports, at the decreeing of mobilisation the railways were able to execute all the transports, also maintaining civil trains in circulation. As soon as the occupied territory became free, the transport crisis began to feel more and more accentuated, on the one hand, due to the lack of locomotives and materials, the lack of fuel, and on the other hand due to the damages done by the enemy in the occupied territory[24].

Despite all these material difficulties, the morale of the population both in the free territory and in the occupied territory, which now was freed, after almost 2 years of terror, changed for the better; the population responded immediately to the second call[25].

The 2nd mobilisation of the Romanian army, as a whole, cannot be considered as a mobilisation itself because of the political and military situation. It was made only partially, both in the number of large units and as strenght. Indeed, if by the time the 2nd mobilisation was decreed, both the military and the political situation required the re-entry of Romania into the war and therefore the mobilisation of all its forces, then after the conclusion of the general armistice, a general mobilisation itself was no longer justified and that is why the Romanian General Headquarters only proceeded to a reorganisation of the large units and to operations to increase and complete the number of personnel, in relation to the more or less threatening situation of the neighbours. This increase in personnel was required by imperative operational needs, namely: 1) Guaranteeing the Nistru border, against any action by Russian Bolshevik troops or bands. This was all the more important now after the end of the general armistice, when the Austro-German occupation troops in Ukraine withdrew into their homeland; 2) Occupying and enforcing order in Dobrogea where Bulgarian gangs terrorised the Romanian authorities and population; 3) Protecting the Romanian population in Transylvania against the crimes and robberies of the Hungarian regular and irregular armies as well as stopping

[24] *Ibid*, p. 112.
[25] *Ibid*, p. 113.

the Hungarian provocations. In these conditions, the 2nd mobilisation – its preparation and declaration – can be considered as a mobilisation only in the initial phase, and the phase that follows after the conclusion of the general armistice should only be considered as an operation to increase the number of personnel[26].

This increase in personnel continued as long as the operational needs of Transilvania and Hungary required it until the achievement of our national and territorial aspirations.

BIBLIOGRAPHY

1. ***, Romanian Military Archives/Arhivele Militare Române (AMR), *Great General Staff* Collection.
2. Daniel Silviu Niculae, *1918. Reintrarea României în Război*, Editura Mii de cărți, Bragadiru, 2018.

[26] For more details, see Daniel Silviu Niculae, *1918. Reintrarea României în Război*, Editura Miidecărți, Bragadiru, 2018.

ROMANIAN NAVY OFFICERS SENT TO STUDY ABROAD (1925-1928)

Marius-Laurențiu ROHART
Director of the Romanian Navy Museum, Constanța, Romania

Despite the fact that the Navy School was established in Constanța, in 1920, the Romanian Navy considered necessary to send several young officers to study at the Naval Academies in the West. This practice was implemented in the 19th century and many famous officers, some of them even Navy Commanders, graduated from Naval Academies in the West. The present study focuses on a group of young officers educated and trained in Italy and France, starting in the mid '20s. Studying their reports sent to the Navy Inspectorate in Bucharest, interesting lessons are emphasised, which were implemented when they came back to the country. From concepts, through naval tactics, to complex exercises, each officer belonging to the group could acquire certain skills, depending on the specifics of the Navies of the countries they studied in. Once they returned to the Romanian Navy, the officers could promote the acquired information, which had important effects on the Romanian naval thinking during the interwar period.

Keywords: Navy, interwar period, Naval Academy, naval tactics, naval doctrine.

INTRODUCTION

At the beginning of the 20th century, it was considered that the most effective way to maintain contact with the Western naval achievements was to send young officers to study abroad. In the *Report no. 13719* on 28 March 1923, the Chief of the Naval Technical Inspectorate, Rear Admiral Niculescu-Rizea, requested the Council of Ministers to approve to send Romanian naval officers to study abroad. The report showed that the naval attaches of the mentioned foreign countries provided information and relations about the availability of their own governments to receive Romanian naval officers in the academies of Italy, France or Britain, namely in Livorno, Brest or Keyham.

The French authorities proved to be the most open to discussions and they quickly agreed to this proposal, but there were other suggestions to the leadership of the Navy, concerning the British Admiralty[1]. The British party was ready to receive, each year, three naval officers having the rank of second lieutenant, at the Royal Naval Engineering College in Keyham. The cost for the classes was 200 pounds for each officer and Bucharest was also required to cover the accommodation and meal expenses.

At the same time the Italian Naval Ministry chose to accept, in turn, three Romanian officers, with 4 high school classes to study in Italy. Two of them were to attend the three-year programme at the Naval Academy in Livorno. The third one would benefit from a practice programme aboard Italian warship. The classes were free and Romania would pay for the necessary materials and equipment.

Of all these proposals the most advantageous one was, of course, the Italian one, more so because the programme was three-year long, a period considered *"indispensable for the formation of good mechanics for the modern Navy"*[2] by the Naval Technical Inspectorate.

INTELLIGENCE MISSIONS IN FRANCE AND ITALY

Not only young officers would benefit from these programmes of foreign study. One of the most important missions was organized at the end of 1924, when the Commander of the Black Sea Division, at the time Read Admiral Vasile Scodrea, and Lieutenant Commander Gheorghe Koslinski were sent in a mission to gather

[1] The National Military Archives of Romania, Microfilm Collection, roll II 2.2758, file 150, c. 233.
[2] *Ibidem*, c. 234.

information in Italy and France. The aim was to collect intelligence about the naval shipyards in those countries, especially concerning the new submarine projects being built there. The Romanian Navy wanted to know the exact characteristics of the new submarine in construction in the West in order to better adapt its own constructions, since none of its current projects were deemed adequate to suit its needs. Of course, taking advantage of this occasion, the Navy got some precious data since the French and Italian authorities were quite open hoping to get favours with a possible client in the East[3].

In Italy the officers were warmly received and they were given all the info they asked, going so far as being allowed to visit the Arsenal of Spezia. The Naval Ministry in Rome even offered some vacancies for Romanian Navy officers to study at the Naval Academy. In Spezia they could inspect the *"Ansaldo"* Shipyards, the battleship *"Cavour"* and the destroyer *"Falco"*. The Romanian officers were also given some data on the new submarines the Italian Navy was building. The impression they took home was that the Italian armament industry had progressed significantly, including the naval one, producing quality ships[4].

In Paris the Romanian officers were well received. Moreover, they were invited to Cherbourg to inspect the submarine *"Requin"*, the newest one in service for the French Navy. The ship had been launched only five months before the Romanian visit and was part of the naval programmes of 1922 and 1923. It was an oceanic patrol boat for the Atlantic. Weighing 947 tons, it was armed with 3 guns (1x100 mm, 2x88 AA) and 10x550 mm tubes[5].

The official talks were focused on the Russian Wranghel Fleet and the danger it posed for the Romania if it were ever returned to the Bolsheviks. That was a very present threat, since in 1924 there were many incidents at the Romanian-Soviet border in Bessarabia. The arguments of Rear Admiral Scodrea were well aimed. He showed that the return of such a significant force in the Black Sea area, according to the conventions of that time, would allow the crossing of any equal-size naval force in the Black Sea. This was clearly in the disadvantage of France, which did not have the naval power to send a fleet there, but could have been an opportunity for Britain, a much larger naval power[6].

[3] The National Military Archives of Romania, *Inspectoratul General al Marinei* Collection, file 28/1924, pp. 196.
[4] In reality, the Italian fleet, though growing since the Fascists took power, was lagging behind its main rival, France. That is why the Italians were focusing on submarine construction, since they were cheaper and easier to build. According to Brian R. Sullivan, *A Fleet in Being: The Rise and Fall of Italian Sea Power 1861-1943*, in *The International History Review*, vol. 10, no. 1, 1988, p. 116.
[5] Henri Le Masson, *Navies of the Second World War: The French Navy*, vol. I, Macdonald&Co., London, 1969, p. 145.
[6] The National Military Archives of Romania, *Inspectoratul General al Marinei* Collection, file 28/1924, p. 197.

Another Romanian naval officer who also visited the two mentioned countries in 1924 was Commander Petre Bărbuneanu, the Commander of the Naval School in Constanța. Although his mission was to observe the workings of the Naval Academies in France and Italy, he was keen on collecting intelligence for the inspectorate. The quest remained; Romanian needed to create a submarine fleet and some information could be gathered from the French and Italian constructors. Italy was in the process of launching submarines of three types.

The first one, of 1,800 tons, was an oceanic boat and clearly not suited for Romania. Of real interest was the 800 tons *"Mameli"* class, of which Italy launched four units (*"Pier Capponi", "Giovanni da Precida", "Goffredo Mameli"* and *"Tito Speri"*), armed with 6x530 mm tubes and 1x102 mm gun. This type would reach 17 nods on the surface and 9 underwater[7] and was deemed suited for the Romanian Navy by Commander Bărbuneanu.

In France, at Brest, the officer took advantage of the naval exercises of the submarine flotilla there in order to inspect the *"Gorgone"* class submarine, *"Hermione"*, built before the war, in 1917. Displacing 500 tons and armed with 8x450 mm tubes and 1x75 naval gun, this boat was very similar to the *"Laubeuf"*, class, meaning its tanks were inside[8]. At Brest Bărbuneanu was presented the latest achievement of the French Navy in submarine construction, the *"Marsouin"*, only a few months from its launch. The boat was of the *"Requin"* class.

Both information and study voyages had a significant impact on the Romanian Navy's own programmes. In the mid '20s the Navy was in full process of servicing new type of ships like submarines and minelayers.

Despite it, in the long term the most benefits were for the young naval officers sent to study abroad because they could get accustomed with the developments in the West and they managed to implement most of them just in time before the Second World War. The study focuses on one of those officers, Horia Macellariu. He studied in France and Italy, following the negotiations with these countries, which were finalized with the acceptance of a limited number of Romanian officers in the respective Naval Academies. Italy chose to receive two Second Lieutenants at the Naval Engineer School of Genova for two years and one Lieutenant for torpedo training at the Livorno Naval Academy for one year. In France Romania could send a Lieutenant to study at the Naval Warfare School in Paris for one year[9].

[7] Bruno Weyer, *Taschenbuch der Kriegsflotten 1928*, J.F. Lehmanns Verlag, Munchen, 1928, p. 82.
[8] Jean Labayle Couhat, *French Warships of World War I*, Ian Allan Ltd., London, 1974, p. 154.
[9] The National Military Archives of Romania, *Inspectoratul General al Marinei* Collection, file 204/1924, p. 112.

HORIA MACELLARIU AND THE RELEVANCE OF HIS REPORTS

The Lieutenant in question was Horia Macellariu, who went to study at the Naval Warfare School in Paris in 1927-1928. As the other officers he had to report regularly to the Naval Inspectorate in Bucharest. Studying his reports, we can observe the kind of strategic and tactical exercises he had to complete in France and the way they could be implemented in the service of the Romanian Navy.

In an analysis of the naval actions in the North Sea during the First World War, Lieutenant Măcellariu studied the objectives and methods used by the German Imperial Navy to ensure its access to the High Seas[10]. The naval operations on the Belgian coast were of interest for the Romanian officer because they could be compared with those undertook by the Romanian Navy in the same period of time. He was focused on two types of operations. On the one hand, the blockade of the Belgian ports of Zeebrugge and Ostende by the Royal Navy. The ports were occupied by the Germans since the start of the war. On the other hand, he looked at the bombing of the Belgian coastline positions by the Allied ships in the later parts of the war.

In the first category, *"with maritime objectives"*[11], the future Commander of the Romanian Navy during the Second World War, Horia Macellariu, included the blockade of the two Belgian harbours by the Royal Navy. The Germans were using these ports as staging grounds for supply ships for their High Seas Fleet, but also as bases for their submarines and hydroplanes, which were threatening the South coast of England. That was actually the reason why the Royal Navy wanted to cut the threat at its roots and annihilate the submarines in their protective bases. We see here a first parallel with the situation of 1939-1945, when the annihilation of the German submarine bases was one of the main objectives. This took many forms in the Second World War, but the aim was always the same: the neutralization of threat posed by those ships for British communication and supply lines. The basic principle the British planned to employ was one of *"strategic speed"*, which meant they had to destroy the submarines before they could do any damage. It required their destruction or at least blocking their bases of operations.

As in the case of the Second World War, the Germans protected their submarines with powerful concrete structures so the only viable solution was to block the harbour. It was not an easy task because the German coastal defence was equally formidable: over 200 guns, of 150-300 mm calibre, spread out on the coast. The dike at the entrance of the Port of Zeebrugge had torpedo tubes for protections, a stockade made of barges and torpedo nets.

[10] *Ibidem*, p. 764.
[11] *Ibidem*.

The British plan was to use their monitors and airplanes to bomb the area for a couple of days, so that the defenders could be kept in the dark concerning the real date of attack. Moreover, they set up a diversionary attack on the dike, all the while their focus being on the harbours of Ostende and Zeebruge, by blocking the canals there[12].

These operations were an important success for the Royal Navy both *"materially and psychologically"*, because the ports had to be closed for a long period of time. In the case of the enemy morale, the fact that the British were capable of mounting such a serious attack, with over 100 ships, severely damaged the morale of the German defenders[13].

The success of these raids was owed mainly to the efficient coordination of different services of the Armed Forces. The element of surprise was also a contributing factor. We should also acknowledge the fact that the British Admiralty took a calculated risk with this operation. An important factor was represented by the excellent communications between the ships, the British could this way keep in touch with both the attacking forces, one for each harbour. Another lesson that the Romanian officer was able to use from this attack was the great importance of the coordination between the Land Forces and the Navy, because the Army's artillery could also act as another distraction for the enemy[14].

Lieutenant Macellariu noticed that, in general, the training of the men involved in this kind of high-risk operation was crucial. *"Well drilled, prepared and motivated men"*[15] were an important factor, because they had better morale and they believed in the success of the operation: *"Each men knew what he could expect from the attack and still had hopes of coming back alive, because he knew that every measure was taken to ensure his rescue with fast boats, for example. It is not good to go to war with men that know they are not coming back"*[16].

Another interesting perspective, which was very useful in the case of a naval war in the Black Sea area, was the cooperation with the Air Force. In his report to the Navy General Inspectorate, Macellariu argued that *"one could see the significant influence in future naval operations"*[17].

In respect to the landing operations, which were quite useful as seen in the Black Sea area between 1941 and 1944, the British raids on the Belgian coasts showed some interesting conclusions. First of all, one would have to use different

[12] *Ibidem*, p. 766.
[13] *Ibidem*.
[14] *Ibidem*, p. 767.
[15] *Ibidem*.
[16] *Ibidem*.
[17] *Ibidem*.

types of ships, with monitors (or battleships), armed with heavy artillery that could soften up the enemy coastal defences. Then destroyers would have to come into play, followed up by torpedo boats. Here the Romanian officers noted correctly that those small boats could act as a defence screen for the big gun ships while they were pounding the enemy batteries on shore. It proved to be a correct assessment in the Second World War, examples in this regard being the Soviet Black Sea Fleet landings in Crimea, in the winter of 1941-1942.

Another interesting conclusion of Lieutenant Macellariu in France was about the different elements forming the coastal defence force. Although the Germans had significant assets on the ground, both in men and materials, including a great number of artillery pieces, without good, reliable intelligence, they were exposed to the Allied attack. As it happened in 1944, in Normandy, which was a couple of hundred miles to the south of the Belgium coast, the air and naval superiority of the invading force prevented any patrols from alerting the Germans of the impeding attack[18].

In respect to the support that the Navy's big guns could offer to the Army, Lieutenant Macellariu noticed that in the First World War, the naval operations on the Belgium coast could be categorized into two parts: those in the first years of war and then those in 1918. In the beginning the Allies made good use of their naval superiority in the Channel to bring in warships of different tonnages, especially light destroyers and even gunboats to attack the German coast. The enemy reacted with the fortification of its coast and the installation of coastal artillery. The Admiralty used bigger ships which proved to be dangerous for the battleships, cruisers and destroyers. If we add to this the danger of torpedo attacks form the enemy submarines, we can clearly see that the British ships were quite exposed to many perils and their accuracy suffered as a consequence, all the while being in range of the enemy coastal guns. More so, the smaller ships were also used to bomb the enemy positions and had to go back to defend their bigger counterparts[19].

CONCLUSIONS

All of the mentioned considerations made the development of a new type of warships – the maritime monitor inevitable. Armed with heavy artillery, this ship could tackle the German batteries and because it had a low draught, it could get quite close to the coast to increase its accuracy. Furthermore, it had torpedo tanks, partially filled with water, so that it was almost impervious to torpedo attacks.

[18] *Ibidem*, p. 768.
[19] *Ibidem.*

These ships were used to bomb the German coastal positions in the second phase of the operations, in 1918. The attacks yielded better results than those of 1915-1916. Lieutenant Macellariu observed that those raids caused *"serious concern"* for the defenders. The main conclusion of his study was that the age of *"squadron ships"*, all-rounders, that could fulfil all range of missions was over. They were replaced by specialised warships, and, very soon by aircraft[20].

BIBLIOGRAPHY

1. ***, National Military Archives of Romania, *Inspectoratul General al Marinei* Collection.
2. Jean Labayle Couhat, *French Warships of World War I*, Ian Allan Ltd., London, 1974.
3. Henri Le Masson, *Navies of the Second World War: The French Navy*, vol. I, Macdonald&Co., London, 1969.
4. Brian R. Sullivan, *A Fleet in Being: The Rise and Fall of Italian Sea Power 1861-1943*, in *The International History Review*, vol. 10, no. 1, 1988.
5. Bruno Weyer, *Taschenbuch der Kriegsflotten 1928*, J.F. Lehmanns Verlag, Munchen, 1928.

[20] *Ibidem*, p. 769.

GHEORGHE DABIJA – SOLDIER, DIPLOMAT AND WRITER –

Gabriel-George PĂTRAȘCU, PhD
National Military Archives of Romania, Bucharest

Gheorghe Dabija became known in the Romanian military journalism through his studies and works of military pedagogy, where he approached various aspects of the training and education of the troops. Within the period 1910-1913 he was a military attaché in Sofia and Belgrade. He participated in the Reunification War 1916-1919, commanding different military structures, a fact that enabled him, after the finalization of the military operations, to dedicate himself to the military history, drafting an exceptional monography dedicated to the battle actions developed within the period 1916-1918.

Keywords: Brigadier General Gheorghe Dabija, First World War, Romanian military writer, military attaché.

MILITARY ACTIVITY

Gheorghe Dabija was born on 20 September 1872 in Iași, being the son of Alexandru and Natalia, and he died in Bucharest, in 1957. Born within one year after the marriage of his parents, he received a higher, thorough education, in the spirit of the responsibility towards life, devotion to the ancestors and supreme respect due to the country[1]. On 16 July 1891, he was enrolled at the Officer Training School, which he graduated on 16 July 1893 with the military rank of Second Lieutenant. His military ranks were as follows: Second Lieutenant (16 July 1893), Lieutenant (08 April 1896), Captain (28 November 1902), Major (10 May 1910), Lieutenant Colonel (01 April 1916) and Brigadier General (01 September 1917).

In 1893, he graduated the Officer Training School with the military rank of Second Lieutenant and on 16 July he was assigned to the 4th Hunter Battalion. He remained in that elite unit until 08 April 1896, when he was transferred to the 13th Regiment *"Ștefan cel Mare"*, a unit where he received the rank of Lieutenant. After one stage in this regiment, he returned to the 4th Hunter Battalion, from where, on 01 November 1902 he entered, only for a few days, in the structure of the 2nd Regiment *"Vâlcea"*. On 28 November 1902, he was transferred to the 31st Regiment *"Calafat"*, and on that date he was advanced to the rank of Captain.

It must be mentioned the fact that the transfers took place only in documents because, in reality, within the period 18 September 1901 – 01 October 1903, Lieutenant, and since 1902, Captain Gheorghe Dabija was *"attached for service in the Austro-Hungarian army".*

On 01 April 1904, he returned, only for one year, to 4th Hunter Battalion, and on 01 April 1905 he was transferred to the 3rd Division which was quartered in Târgoviște. He activated in that large unit for one year and on 01 April 1906, through the High Decree No. 1516/1906, he entered in the structure of the Firing Training School.

The series of the work-related transfers continued one year later when, on 01 April 1907, through the High Decree No. 1789/1907, he was transferred to the 14th Regiment *"Roman"*. In his journey through the units he activated in he was appreciated by his commanders, a reason why, on 22 October 1907, through

[1] Delia Bălăican, *Generalul G. A. Dabija – un reprezentant de marcă al generației sale*, in the Scientific Annals of *"Alexandru Ioan Cuza"* University, Iași, History, LXI (2015), Editura Universității *"Alexandru Ioan Cuza"*, Iași, 2015, p. 395.

the High Decree No. 3527/1907, he was detached to the Great General Staff. After a one-year stage, on 25 October 1908, through the High Decree No. 2907/1908, he returned to the 14th Regiment *"Roman"*, where he filled various staff positions.

On 01 October 1909, through the High Decree No. 2769, he was once again detached to the Great General Staff where, on 10 May 1910, through the High Decree No. 1775/1910, he was advanced to the rank of Major, a very special moment in the military career of the future General.

The activity of Major Gheorghe Dabija in the command structures of the Romanian Armed Forces continued also in the following years. Therefore, on 01 October 1913, through the High Decree No. 5860 on 07 November 1913, he was transferred to the 1st Infantry Department within the Ministry of War where he fulfilled various general staff positions with attributions in the reorganization and coordination of the Infantry branch, under the conditions in which the Romanian general staff began to outline conclusions from the campaign developed on the territory of Bulgaria in July 1913[2].

The date of April 01, 1914 represented one of the most important moments in the military career of the future General. Therefore, through the High Decree No. 1148 on 18 March, Major Gheorghe Dabija was advanced to the rank of Lieutenant Colonel receiving, at the same time, the command of the 2nd Hunter Battalion *"Regina Elisabeta"*.

On 01 April 1916, with only a few months before Romania entered the war together with the powers of the Triple Entente, through the High Decree No. 1024 on 17 March 1916, Lieutenant Colonel Gheorghe Dabija was appointed at the command of the 6th Regiment *"Mihai Viteazul"*, being advanced to the rank of Colonel on 10 May 1916, through the High Decree No. 1863 on 03 May.

On 17/27 August 1916, this unit was subordinated, from a hierarchic point of view, to the 8th Infantry Brigade, under the command of Brigadier General Gheorghe Mărdărescu, the 4th Infantry Brigade, under the command of the Brigadier General Gheorghe Burghelea, 2nd Army Corps, under the command of the Divisional General Dumitru Cotescu and, not lastly, the 2nd Romanian Army, under the command of the Divisional General Alexandru Averescu.

Since the first day of war, the 6th Regiment *"Mihai Viteazul"* participated actively in the Romanian offensive north of the Southern Carpathians, managing, within a short period of time, to liberate Brasov.

The activity from the first part of the war, more precisely the period 14 August 1916 – 01 February 1917, is presented in a statement by Colonel Gheorghe Dabija,

[2] Prof. univ. dr. Valeriu Avram, Lucian Drăghici, Gabriel-George Pătrașcu, dr. Ion Rîșnoveanu, *Războiul de Întregire (1916-1919) Comandanți Militari Români*, Editura Centrului Tehnic Editorial al Armatei, București, 2016, p. 48.

as follows: *"Within the period 14 August 1916 – 01 February 1917, with the rank of Colonel as Deputy Chief of Staff for the 3rd Army and the 2nd Army; Chiefs: General Staff Chief – General G. Mărdărescu; Commander of the 3rd Army: General M. Aslan; Commanders of the 2nd Army: General Gr. Crăiniceanu and General A. Averescu"*.

During the campaign in 1917, more precisely during the battle from Mărăști (9/22 July – 24 July/01 August), Colonel Gheorghe Dabija held the command of the 16th Infantry Brigade, subordinated to the 8th Infantry Division, under the command of the Brigadier General Ioan Pătrașcu, 2nd Army Corps, under the command of the Divisional General Artur Văitoianu, the superior echelon being represented by the 2nd Army, under the command of Army Corps General Alexandru Averescu, as it results from the above-mentioned statement: *"Within the period 01 February 1917 – 01 September 1917, with the rank of Colonel, I held the command of the 16th Infantry Brigade. On 01 September 1917, I was advanced to the rank of General. Within the period 01 September 1917 – 08 February 1918 – General, Commander of 16th Infantry Brigade. Chiefs: Divisional Commander: General I. Pătrașcu; Corps Commander: General Artur Văitoianu"*. From this statement, it results the fact that, on 01 September 1917, Colonel Gheorghe Dabija was advanced to the rank of Brigadier General, in compliance to the High Decree No. 1405 on 01 December 1917.

The year 1918 represented another important reference point for Brigadier General Gheorghe Dabija, to whom it was assigned the command of the 6th Infantry Division. Therefore, *"Within the period 08 February- 01 June 1918 – Commander of the 6th Division. Chiefs: Corps Commander (meaning 3rd Army Corps): General I. Pătrașcu. Within the period 01 June 1918 – 12 November 1918 – Commander of the 18th Infantry Brigade. Chiefs: Divisional Commander: General Alex Atanasiu; Corps Commander: General I. Pătrașcu. Within the period 12 November 1918 – Commander of the 2nd Hunter Division. Chiefs: within the period 12 November 1918 – 14 April 1919, Divisional General Moşoiu Traian. From 14 April – Divisional General Mărdărescu Gheorghe, Commander of the Troops in Transylvania"*.

From the above-mentioned statement, it clearly results the fact that, also after the signing of the Peace Treaty from Bucharest, between Romania and the Central Powers, on 24 April/07 May1918, and also after the demobilization of a part of the Army, Brigadier General Gheorghe Dabija held the command of the 6th Infantry Division, the 18th Infantry Brigade or the 2nd Hunter Division, large units which participated in the campaign from Transylvania and Hungary against the Soviet power instituted by Béla Kuhn[3].

[3] *Ibidem*, p. 49.

In the conditions of the demobilization of the army in the spring of 1920, on 01 July 1920, he resigned and he was removed from active duty according to the High Decree No. 2899 on 10 July 1920, therefore ending a brilliant career in which Brigadier General Gheorghe Dabija proved his military and command qualities, and also his bravery and heroism, until the finalization of the actions in Hungary and the decree of demobilization.

Along his military career, Gheorghe Dabija enjoyed the appreciation of his direct commanders, a fact that proves once again the human and military quality of the officer. In the Qualifying Sheet for 1916 (within the period 15 August 1916 – 15 February 1917), Brigadier General Gheorghe Mărdărescu, the Chief of Staff of the 2nd Army, stated: *"Colonel Dabija Gheorghe acted as Deputy Chief of Staff of the 2nd and 3rd Armies, until 15 February 1917. Intelligent, well-prepared, with a formidable labour capacity and very thorough in his work, he was a precious collaborator of mine. Colonel Dabija is not only a good staff officer, but he also has a deep insight of Infantry, which makes him and excellent Division Commander. I was very much satisfied with his services – both at the office and also outside it – and he was an example of duty fulfilment for the officers from the Armed Forces Headquarters".*

In 1917, Brigadier General Ioan Pătraşcu, Commander of the 8th Infantry Division, characterized Brigadier General Gheorghe Dabija, in a eulogistic manner, as follows: *"General Dabija was advanced in November. Beginning with that month until now, he continued to command the 16th Brigade in the same good conditions. In that period, he controlled the organization of his sector in good conditions".*

One of the most beautiful characterizations in his military career was offered by the Divisional General Traian Moşoiu, the Commander of the troops from Transylvania, who, on 01 April 1919, stated: *"He controls the 2nd Hunter Division. Even if the Division was set up at the moment of the mobilization, General Dabija, through his hard work and special skills, managed, through restricted means, to organize the unit in the best conditions. In the occupation area, assigned to the Division, it was re-established and maintained the order, in a strong manner, and on the Zam – Baia de Cris line, the troops of the Division performed their duty in a great manner. General Dabija had successfully handled the improvement of the unit training, setting up a training centre, organized in excellent conditions, leading to very good results. Considering the fact that we are in the situation of very important military operations, I reserve the right to characterize him after the finalization of these operations. I propose him for the awarding of the Order "Steaua României" (Romanian Star) with swords to the rank of Commander with a cordon of "Virtutea Militară" (Military Virtue), for his merits in the occupation of Transylvania"*[4].

[4] *Ibidem*, p. 50.

DIPLOMATIC ACTIVITY

Bulgaria was the third state where Romania decided to send a military attaché, after Germany and Austria-Hungary. The first military attaché accredited at Sofia was Captain Nicolae Petală, in 1904, followed by the Captain Gheorghe Dabija, at that moment, the Chief of Cabinet of the Minister of War. Through the quality of his reports, based on the analysis of the information from open sources, the military attaché in Sofia had the possibility to directly influence the policy of the Romanian authorities. His activity was strictly monitored by the Bulgarian Intelligence Service. Sensitive to any information that could affect his statute of military attaché, Gheorghe Dabija rejected any accusations of espionage brought against him[5].

Irrespective of the nature of his sources, Gheorghe Dabija was the only Romanian military diplomat able to find out, through his own efforts, information about the negotiations between the Balkan states for the establishment of the Balkan League. On 14 April 1912, he presented to King Carol I, the text of the alliance treaty between Bulgaria and Serbia and its secret appendix, both signed at the end of February. Major Gheorghe Dabija developed his activity as military attaché in Sofia, starting on 10 May 1910 until 1913, when he was sent to Belgrade, also as military attaché, fulfilling this position until 1914.

About the military diplomat mission, Gheorghe Dabija stated as follows: *"I loved my country and everything I did as a military attaché, I did only to its superior interest, according to the instructions received from the Ministry of War, the Great General Staff and, especially, His Highness King Carol I, who honoured me with his trust. My conscience was and remained also today, after 35 years (1910-1945) completely calm and at peace"*[6].

SCIENTIFIC ACTIVITY

Brigadier General Gheorghe Dabija valued through writing his professional experiences, from the training stage in Austria-Hungary, within the period 1901-1903, until the activity of military diplomat in Bulgaria and Serbia, within the period 1910-1913, or through the effective participation on the battle field during the Reunification War (1916-1919). The military writings marked his life, offering him a maximum freedom of expression, but also causing him the worst prejudices, representing the head of claims of the communist courts, Gheroghe Dabija being imprisoned in Jilava and Văcărești penitentiaries, within the period 08 August 1952 – 18 January 1955.

[5] Delia Bălăican, *op. cit*, p. 401.
[6] *Ibidem*, p. 402.

The books and articles having military thematic, written by general Dabija, came to the fore through the direct reference to the practical aspect of the training of the troops, through concision and the comparative study of the works regarding the instruction of the large armies of the world and universal history, through the understanding capacity of the human resorts which determined the military or political decisions, affecting the future of a country[7]. The specialists within the Romanian Academy Library identified five categories of works of Gheorghe Dabija:

- **Books and articles of history and military diplomacy:**

a. Books regarding the Balkan Wars: *"Războiul bulgaro-turc din anul 1912-1913"*, a book that received from King Carol I the medal *"Bene Merenti"* 1st class, of gold, in 1914, and the Romanian Academy awarded him the Prize *"Adamache"*, based on the report of Nicolae Iorga. The first book about Southern Dobruja, *"Cadrilaterul Bulgar/Bulgarian Quadrilateral"*, which appeared with only a few weeks before the entry of Romania in the Second Balkan War[8].

b. The topic – First World War – *"Armata Română* în *Războiul Mondial (1916-1918)"*, written in four volumes, within the period 1928-1937, his most valuable book, a reference work in the bibliography of the First World War[9]. The work *Armata română* în *războiul mondial 1916 – 1918* has a great documentary value. It contains a rich factual material – starting from the orders of the Great General Headquarters, operative orders of the armies and divisions, to phone calls between the officers from the armed forces staffs – enabling the analysis and understanding of the complex mechanism of the organization and command of the military actions of the different echelons, the existing relations between commands and commanders, the used methods and procedures, the manner in which the units and the large units of the Romanian Army fulfilled their battle missions. This work presents fewer aspects with respect to theoretical, strategical and tactical appreciations, regarding the development of the military actions[10]. The work contains both a detailed description, based on archive documents, of the military operations and a severe analysis of the deficiencies and errors resulting in the Romanian troops being defeated in the battlefield[11].

The author, a direct participant in those events, adopted a critical tone, the value judgements regarding certain commanders being very severe.

[7] *Ibidem*, pp. 396-397.
[8] *Ibidem*.
[9] *Ibidem*, p. 398.
[10] *** *Istoria Gândirii Militare Românești*, Editura Militară, București, 1974, p. 252.
[11] Prof. univ. dr. Valeriu Avram, *op.cit*, p. 50.

Therefore, Gheorge Dabija had critical appreciations regarding the operation plan of the Romanian command. The *"Z"* Hypothesis, because of his less manoeuvre character. The author considered that a strong blow performed together with the Russian Army in Bucovina would have been more indicated, and that would have returned the defence of the enemy from the Transylvanian Plateau and Galicia. Also, the author, in consensus with the opinion of General, future Marshall Alexandru Averescu, minimalized the role and importance of the battle from Mărășești, which was not considered by them to be a proper operation, according to the canons of the military art. On the contrary, the battle from Mărăști was a model of organization and execution, having a particular success. In that case, Gheorgeh Dabija was unfair and biased, his appreciations being subjective, resulting from his admiration towards Alexandru Averescu and antipathy against General Constantin Prezan[12].

The foreword of the work was signed by Marshall Alexandru Averescu, former commander of the author, who stated: *"General Dabija, with the pen in his hand, was the officer who participated in the war and his thinking manner reflected in his writings was different from the thinking manner during the war only through the fading caused by the passage of time, meaning the period of time from the operations and their description. Therefore, in the valuable work of General Dabija, additionally to the material gathered with an exemplary diligence, we could also find the interpretation of the various events occurred before his eyes or around him, observed in the light of the cruel reality, with the undefeated dreams of the officer willing to serve his country"* [13].

c. Military Chronicles of the Second World War appeared in the newspaper *"Curentul"* (25 June 1943 – 23 August 1944).

- **Military writings about the instruction of the Infantry troops**. 11 works are part of this category, some of them being re-edited, the most appreciated one being *"Instrucția practică a companiei de infanterie*" (1904), to which we may add the articles edited in *"Revista Infanteriei"* and *"Revista Armatei"*.
- **Works based on which it was set up and operated the National Staff School** [Superior War School – n.n.]. The most conclusive example is represented by *"Regulamentul de manevră de luptă al infanteriei"* (1910), based on which

[12] Dr. Petre Otu (coordinator), *Personalități ale Gândirii Militare Românești*, Editura Academiei de Înalte Studii Militare, București, 1997, pp. 138-139;
[13] General G. A. Dabija, *Armata Română în Războiul Mondial (1916 – 1918), 1st Volume*, Editura IG. HERTZ, București, 1937, pp. 10-11.

the Romanian Armed Forces were upgraded to the standards of the modern armies of the world.

- **The motivational writings** through which he directly pleaded the unfading principles and values, like: truth, dignity, patriotism. We can mention here the work: *"Dresaj sau educațiune?"* and the articles from *"Revista Infanteriei"*: *"Patriotismul nostru*, *Tactica aplicată – marș, staționare, luptă"*, to which we may add his memoirs.
- **The memoirs** represented by the innovative work, *"Amintiri din cariera militară (1893-1920)"*, *"Oameni, tipuri, obiceiuri, năravuri"* and *"Sisteme de altădată"* (1945), in the patrimony of the Library of the Romanian Academy. The about 700 pages help us to discover the contemporary period of the author, the personality and career of General Gheorghe Dabija. The volume published in 1936 is added to this work – *"Amintirile unui atașat militar român* în *Bulgaria 1910-1913"*[14].

The analysis performed by the author regarding the German-Polish War in September 1939 is also useful. Presenting the mutations of the military organization and technique, Gheorghe Dabija considers that the total war, materialized by the German army in the case of Poland, was envisaged in all countries and it shall form the army conflict in the future[15].

CONCLUSIONS

Brigadier General in reserve, Gheorghe Dabija is one of the most important Romanian military thinkers. He had the chance of a career that can hardly be equalled or outperformed even in the present days. He was a career soldier and he commanded military structures up to division level, participating with them in battle actions. He pursued a career in the military diplomacy field, as a military attaché and he excelled in the military journalism field. Unfortunately for the Romanian historiography, the work dedicated to the participation in the campaign from 1919, when he was at the command of the 2nd Hunter Division, and participated in the battles against the Hungarian army, was not published. Through his entire theoretical activity, Brigadier General Gheorghe Dabija, was an original thinker, who refused to follow the easy way of taking-over certain ideas and solutions, already prepared, seeking to promote modern methods and modalities of instruction and of analysis of the military phenomenon[16].

[14] Delia Bălăican, *op. cit*, p. 398.
[15] Dr. Petre Otu (coordinator), *op. cit*, p. 139.
[16] *bidem*, p. 142.

BIBLIOGRAPHY

1. ***, National Military Archives of Romania, *DCI/Memorii. Bătrâni/Generali/litera D, generali Collection*.
2. ***, *Istoria gândirii militare românești*, Editura Militară, București, 1974.
3. Prof.univ.dr. Valeriu Avram, Lucian Drăghici, Gabriel-George Pătrașcu, dr. Ion Rîșnoveanu, *Războiul de Întregire (1916-1919). Comandanți Militari Români*, Editura Centrului Tehnic-Editorial al Armatei, București, 2016.
4. Delia Bălăican, *Generalul G.A. Dabija – un reprezentant de marcă al generației sale*, in Scientific Annals of *"Alexandru Ioan Cuza"* University, Iasi.
5. Generalul G.A. Dabija, *Armata Română în Războiul Mondial (1916- 1918)*, vol. I-IV, Editura I.G. Hertz, București, 1937.
6. Dr. Petre Out (coordinator), *Personalități ale gândirii militare românești*, Editura Academiei de Înalte Studii Militare, București, 1997.

GENERAL IOAN DUMITRACHE, PORTRAIT OF A LEGEND
COMMANDER OF THE 2ND MOUNTAIN DIVISION – "DIVIZIA DE CREMENE"

Florian BICHIR, PhD
Lecturer, "Carol I" National Defence University, Bucharest

The activity and the memoirs of General Ion Dumitrache are undoubtedly important, if not capital, for knowing our history and especially the history of the Second World War. It is notorious that Mountain Troops represented the only elite troops of the Romanian Infantry during the entire Eastern Campaign. In today's jargon a kind of "green berets". The best known of them was the 2nd Mountain Division.

The courage of the fighters under the command of General Dumitrache made the 2nd Mountain Division to acquire on the front a well-deserved renown, in sync with the determination demonstrated by the troops of that great unit: "Divizia de Cremene". Historian Alesandru Duţu noted in his most recent volume that "General Dumitrache led large units of the Romanian Army that reached the easternmost point in the Second World War. The Romanian troops under his command fought in the Caucasus Mountains, the 2nd Romanian Mountain Division reaching close to Grozny, the capital of Chechnya!"

Keywords. Second World War, General Ioan Dumitrache, 2nd Mountain Division, Crimea Division, Grozny, Chechnya.

INTRODUCTION. BIOGRAPHY. MILITARY EDUCATION AND TRAINING

The future general was born on 25 August 1889[1], the same year as his future comrade-in-arms, General Leonard Mociulschi[2], in Slobozia - Ciorăşti, as the only child of Gheorghe and Ioana Dumitrache. *"The undersigned Dumitrache Ion was born on 25 August 1889 in Ciorăşti, R. Sărat County, son of Gheorghe and Ioana (dead). I attended the primary school in the village of Cîorăşti, the gymnasium in Râmnicu Sărat and the high school "Alexandru Ioan Cuza" in Focşani"*, as confessed in an autobiography before the *Securitatea*[3].

He attended the gymnasium in Râmnicu-Sărat and the high school in Focşani.

In 1909 he was admitted to the Military School of Infantry Officers in Bucharest, which he graduated on 15 June 1911, with good results, being advanced to the rank of Second Lieutenant. The young officer began his military career on 1 July 1911 in the 38th *"Neagoe Basarab"* Infantry Regiment of Braila. For three years he ambitiously trained the recruits he commanded in the Second Balkan War (17/30 June – 17/30 July 1913)[4].

---

1 Valeriu Anghel, Alexandru Deşliu, *Voca*ţie şi destin*. 600 fi*şe-portret pentru un tablou spiritual-istoric al judeţului *Vrancea*, Editura Terra, Focşani, 2000, p. 115.

2 Leonard Mociulschi (1889 - 1979). He participated in the Campaign of Romania in the Balkan War (1913), but also in the First World War, noting in the battles of Oituz and Soveja, for which he was decorated by both King Ferdinand and General Berthelot. In the Second World War, Colonel Mociulschi was noted as Deputy Commander of the 1st Mountain Joint Brigade forcing the Dniester, for which he was decorated with the *"Mihai Viteazul" Order*, 3rd class, in the rank of Knight (High Decree No. 2,886/17 October 1941). Promoted to the rank of Brigadier General (1942), he was appointed Deputy Commander of the 4th Mountain Troops Division, a unit noted in the Sevastopol area offensive. In the same year, he was promoted to the command of the 3rd Mountain Division, which led to heavy fighting with the Soviets in the Taman-Caucasus area (until August 1943 when it was withdrawn in Crimea for restoration). Brigadier General Mociulschi was decorated with the *Order "Mihai Viteazul" - 2nd class* (Royal Decree no. 382/19 February 1944). After 23 August 1944, General Mociulschi was appointed at the command of the *"Crişuri"* Group, participating in the liberation of Western Transylvania. Its division participated in the liberation of Hungary, reaching as far as Slovakia. The victories from the Javorina massifs brought to the Division General, Leonard Mociulschi, the *"Mihai Viteazul" 3rd class Order, with swords*. The end of the war found him at the command of the Mountain Corps. When the Communists came to power, he was arrested and imprisoned without trial (1948 - 1964). It was rehabilitated at the intervention of the President of France, Charles de Gaulle, in 1966 (Gheorghe Suman, *Vânători de Munte* in *Enciclopedia Armatei României*, Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009, pp. 184-188; Eugen Stănescu, Iulia Stănescu, Gavriil Preda, *Cavaleri ai ordinului "Mihai Viteazul"*, Editura UNIVERSAL CARTFIL, Ploieşti, 1996, pp. 342, 344, 459).

3 Archive of the National Council for Security Studies (ACNSAS), Criminal Collection, P 076544, Vol. 1

4 Horia Dumitrescu, Marilena Sima, *General de corp de armată Ion Dumitrache (1889 - 1977). Contribu*ţii, *"Cronica Vrancei"* XIX, Vrance Museum, 2014, pp. 369-393

He was advanced to the rank of Lieutenant in 1914, and between 1914 and 1916 he was trained in infantry and military and professional specialization[5]. He participated in the First World War from August 1916. He was noted in the battles from Mărășești - Răzoare (August 1917), being wounded, decorated and advanced to the rank of captain (1917)[6]. He was admitted to the Superior War School[7] in 1919 (it was 30 years since the establishment of the prestigious educational institution in the Romanian army), which he graduated on 10 October 1921 with an average of 6.78 and the qualification *"Good"*.

Promoted to the rank of Major (1920), after graduating from the Superior War School, he was assigned as a Chief of Staff in the Command of the 1st Mountain Troops Division in Arad, which included all the troops of mountain hunters.

By the Decree no. 1,674/1 August 1924, the Command of the Mountain Hunters Corps was transformed into the Mountain Hunters Corps, located in Bucharest. Also, the 1st Mountain Troops Sinaia and the 2nd Mountain Troops Bistrita - Năsăud were set up[8]. Advanced to the rank of Lieutenant Colonel, he was promoted, in 1927, Deputy Commander of the 1st Mountain Division. After two years he was appointed Commander of the 2nd Mountain Troops Battalion in Caransebeș. From the autumn of 1931, Lieutenant-Colonel Ioan Dumitrache worked in the General Staff of the Territorial Inspectorate of Bucharest[9].

The special qualities of Lieutenant Colonel Ioan Dumitrache were confirmed by the characterizations made by his superiors. We exemplify through the Qualifying Sheet for the period 1 November 1930 – 31 October 1931:

Colonel Savu: *"Lieutenant Colonel Dumitrache Ioan commanded from 1.II.930 to the day X 931 the 11th Mountain Troops Battalion – which was independent.*

Physical aptitudes: As in 1929/30.

Military skills: As in 1929/30.

Capacity: As in 1929/930. With the following additions. Through serious studies he has enriched both his professional and general knowledge.

Military education: As in 1929/30.

[5] Constantin Chiper, *General de corp de armată Ion Dumitrache*, in *Veterani în slujba Patriei*, vol. II, under the aegis *of the National Association "Cultul Eroilor"*, Editura BURATINO, Ploieşti, 2006, p. 7.

[6] *Ibidem*, p. 8.

[7] The Superior War School was established on the basis of Decree no. 2,073/8 August 1889. The duration of the courses was two years. Its activity was interrupted during the First World War, the institution resuming its courses on 1 March 1919 (Florian Râpan, Dorel Buşe, *Învăţământul militar*, in *Enciclopedia Armatei Române*, Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009, p. 994).

[8] Constantin Chiper, *op. cit*., p. 8.

[9] *Ibidem*, p. 9.

Service fulfilment: He performed the service as well. As a Corps Commander with a lot of zeal, very conscientious, with a great deal of self-sacrifice having the most beautiful results.

The battalion commanded by him is well trained, well disciplined and well managed. Lieutenant Colonel Dumitrache led the training and education of the officer corps and of the re-engaged personnel with good results. -

This year the ski patrol took the 3rd prize in the CMV competition.

He continued to remove the shortcomings regarding the troops accommodation, and to take care of the war material with good results. -

Through his care a large hut was built in the mountains for 150 soldiers and officers who would bring great profits for mountain instruction.

For the applications in the garrison, he successfully commanded the Infantry Regiment, with artillery, proving that he knows how to well conduct a detachment on the tactical field.

He has often proved to be a very correct referee. -

The officer leaves the battalion command after 2½ years to continue his specialization as an officer.

Conclusion: very good and reliable front and staff officer, who deserves to be entrusted with the leadership of a group of mountain troops.

Not having the necessary seniority this year, he is not the subject of a proposal".

Colonel A. Phlepps – Commander of the 1st Mountain Troops Brigade: *"I totally agree with the note given by the group commander.*

At all the inspections I carried out at this Battalion during the training hours I found this officer remarkably in his place as a commander of a separate corps.

Full of zeal and skill, he led instruction and practice with great talent and and kindness, so this battalion took the lead of the Brigade. -

He commanded the battalion in difficult mountainous terrain, during difficult atmospheric conditions, in the most beautiful way taking the most accurate decisions, achieving them with remarkable energy, and being praised by the General Inspector who was present.

Lieutenant Colonel Dumitrache is a very valuable commander and demonstrating rich professional knowledge, being independent and apt to command a regiment (Mountain Troops Group).

He is a superior officer with all the aptitudes for the activity in the mountains, being a remarkable mountaineer, who animated his subordinates in this direction. -

Not having the necessary age, he is not the subject of a proposal"[10].

[10] Military Archives Vrancea, General Ioan Dumitrache Collection, p. 2.

General Nicola – Commander of the 1st Mountain Troops Division:

" I agree.

Lieutenant Colonel Dumitrache is a mountaineer, a cross-country skier and a peerless instructor. -

He puts soul and passion into training his unit and keeps it always in front of others.

The battalion he commanded excels in outfit, discipline, instruction and shooting.

Lieutenant Colonel Dumitrache personally sets the tone. The first one on the mountain where he built a hut with great sacrifices, first in ski, first in shooting.

His team was awarded in all competitions.

During the Inspection of General Cihosky, he commanded the detachment in the Muntele Mic (South of Caransebeș) at 1,800 altitude. He well appreciates the land and he is perfectly identified with the operations in the mountains. -

He is an excellent mountain officer".

General Gorsky – Commander of Mountain Troops Corps:

"I maintain without reservation the excellent appreciation given by the hierarchical chiefs.

A senior officer who stands out through his entire military achievements, as Corps Chief.

He will be advanced following eligibility".

General Gorsky – Inspector General of the Army:

"I maintain the favourable appreciation given to this valuable senior officer. -"[11].

Advanced Colonel in 1935, he commanded with great firmness the 4th Group Mountain Troops from Bistrița-Năsăud. In the civil hierarchy, Patriarch Miron Cristea (Prime Minister of the country between 11 February 1938 – 6 March 1939) appointed him in 1938 - 1939 as the Prefect of Năsăud County.

He was promoted Commander of the 2nd Mountain Joint Brigade in the autumn of 1939.

Prince Nicholas, the son of King Ferdinand and Queen Mary, set up a Group of 15 officers from the best skiers from the 2nd Mountain Troops Brigade, who were making trips to the mountains when time allowed. On 16 January 1940, Colonel Ioan Dumitrache received the following *Convocation:*

"These 15 will meet this year on 24 January at 10 a.m. in Predeal, Park Garden, from where they will depart to Mount Dihamu.

[11] *Ibidem,* p. 2 verso.

You are urged not to miss the meeting, for which purpose the hierarchical authority was informed in order to be granted a three-day transfer.

Secretary, Major Emilian *Teacă"*[12].

On 10 May 1941, Colonel Ioan Dumitrache was advanced to the rank of Brigadier General[13].

From 20 June 1941, the Mountain Corps commanded by Division General Gheorghe Avramescu passed, operatively, under the command of the 11th German Army.

The mountain troops brigades entered the Holy War on 2 July 1941, attacking the main direction of Rădăuți - Cernăuți - Hotin. The city of Cernăuți was liberated on 4 July 1941. Within these actions, the 2nd Joint Mountain Brigade, commanded by General Ioan Dumitrache, was the spearhead. Together with the 8th Cavalry Division, it forced the Prut and liberated the Land of Herta. By 9 July 1941, the entire northern part of Bukovina was liberated.

Arriving at the Dniester, the *General Antonescu Army Group* ceased its existence and the 11th German Army was subordinated to the *"Southern"* Army Group led by Marshal Gerd von Rundstedt[14], with the mission to advance to the Bug. With great losses, the Bug was crossed, on 21 August 1941. After heavy fighting, the mountain troops crossed the Dnieper on 16 September 1941. The 2nd and 4th Joint Mountain Brigades were disposed on the coast of the Sea of Azov, and the 1st Mountain Joint Brigade was sent to Crimea[15].

By the Royal Decree no. 2,886 on 19 October 1941, Ioan Dumitrache – Brigadier General, Commander of the 2nd Mountain Joint Brigade – was decorated with the *"Mihai Viteazul"* Order, 3rd class.

The human losses suffered, caused the 2nd and 4th Mountain Joint Brigades to be sent to the country (8 November 1941) to complete the numbers, equipment

[12] Military Archives, Vrancea, General Ioan Dumitrache Collection…, p. 3.

[13] Constantin Chiper, *op. cit*., p. 9.

[14] Gerd von Rundstedt (Aschersleben 1875 - Hanover 1953). German Marshal. Chief of Staff of the Division and Army Corps from 1914 to 1918, he was noted as a remarkable organizer. Seeckt's disciple, apolitical, tried to keep his distance from the Nazi regime. Retired in 1938, he was recalled in 1939, when he led the Southern Army Group in Poland, then operated the Sedan attack and the Dunkirk circle. He resigned in November 1941, before invading Ukraine and Crimea. Recalled on the Western Front (March 1942), he was appointed to the command of Army Group D (November 1943). After June 1944, he was replaced by Marshal Hans Günther von Kluge. He led the Ardennes attack since December 1944. Detained by Americans, he was handed over to the English who released him in 1949 (*Grand Larousse en 10 volumes*, Librairie Larousse, Paris, 1993, Volume 9: rectifiable/ *Szymonowic*, p. 2, 710).

[15] More about the military actions in Crimea in Adrian Pandea, Eftimie Ardeleanu, *Românii în Crimeea. 1941-1944, București, 1995.*

and training in peace garrisons, as well as the applications in the mountains. The 2nd Mountain Division (the brigades were transformed into divisions on 15 March 1942) left for the front on 6 July 1942, and on 31 July it was in combat disposition in the Rostov area. Starting on 6 August 1942, the 2nd Mountain Division was permanently subordinated to the German military commanders operating in the Caucasus.

THE VICTORY OF NALCHIK

In the battles in the centre of the Caucasus, the Romanian 2nd Mountain Division (Commander: General Ion Dumitrache) was also engaged, which triggered, on the evening of 22 August 1942, the action of forcing the Baksan River, without artillery training. The surprise did not succeed, because, when reaching the river bank, the units were received by a fiery fire, of all the categories, resulting in great human losses for the Romanian troops. On the ninth day, the attack on the 2nd Mountain Division broke out across the front. The 4th Mountain Troops Group occupied, with battalions 7 and 15, the villages Malka and Kysburun 2, but the enemy resisted, favoured by the configuration of the land. On the night of 23 to 24 August, the 7th Mountain Troops Battalion managed, by a clever manoeuvre, to reach the southern bank of the river, constituting a bridgehead that was kept, despite all the counterattacks executed by the enemy, especially after 27 August. Between 28 August and 31 August, the fights became dramatic, especially in the high zone with the height of 910, which dominated the whole area and through which the road that crossed the Caucasus from north to south passed. It was on the one side or the other for several times.

The heroism of the Romanian hunters was also shown at the assault of quota 910, where Sergeant Rusu, under the command of Lieutenant Botiș, told, looking over his shoulder as he left it: *"Quota 910, dry it God dry it!"*. They were those who survived, who collected on the tent sheets the comrades made pieces by the Soviet artillery, loaded them into trucks, then left, for a new battle for life and death. The Commander of the 1st Company, Captain Tiberiu Coloiu, the superior of Lieutenant Botiș Volumiu, fell with the leg cut from the knees by a shrapnel shell. *"Take the order and resist!"*, he said before being evacuated to the hospital in Piatigorsk, where he died, being buried in the city cemetery[16].

[16] Cristian Negrea, *Vânătorii de munte în Caucaz*, http://cristiannegrea.blogspot.ro/2012/08/vanatorii-de-munte-in-caucaz-i.html, retrieved on 10 September 2019.

Here is the agenda of General Ion Dumitrache after the conquest of quota 910 by the 7th Mountain Troops Battalion:

2nd Division Mountain
Commander

Order of the Day no. 2
On 2 September 1942

In the operations of forcing the Baksan River (Caucasus) and in the bridgehead beyond it on the heights 910 all the soldiers of the division bravely fought. The 7th Mountain Troops Battalion, in the front, surprised the crossing of the river in the village in front of the quota 910, crushed the enemy's defence of the village and entered the heights stormily; thus facilitating the very rapid development of the bridgehead – decisive for the future battle – being mentioned as such in the orders of the Mackensen Armoured Corps. Despite all the heavy losses, although the commander, the deputy commander and all the company commanders were injured, the battalion penetrated and remained steadfastly 10 (ten) days high on the conquered heights, crushing all furious and continually refreshed attacks by the enemy. Thus, it was the backbone of the entire operation. The brave soldiers and officers of the 7th Mountain Troops Battalion deserve unlimited gratitude and admiration, both Romanian and German.

Lieutenant Colonel Ciubotaru Nicolae, the Battalion Commander, though wounded, was in command and with the brave officers remaining, kept his brave battalion on the heights of glory, where he is and must always remain.

He has also shown that he is brave and puts his life in danger for the battalion and the country.

Honour the 7th Mountain Troops Battalion!
The Commander of the 2nd Mountain Division,
General I Dumitrache

On 17 October, the 2nd Mountain Division starts a strong offensive and occupies the entire village of Saiukovo. A day later, General von Kleist comes personally to the heights conquered by the Romanian troops and decorates the soldiers of the Division who have stood out in the battle, declaring: *"The great deed of arms achieved by the Romanian 2nd Mountain Division made possible for the Ist Armoured Army to pass to decisive operations"*[17].

[17] Florin Cristescu, *Operațiunile Diviziei 2 Munte în Munții Caucaz*, http://www.historia.ro/exclusiv_web/general/articol/opera-iunile-diviziiei-2-munte-n-mun-ii-caucaz, retrieved on 10 September 2019.

The German plans provided for the liquidation of the enemy from the Nalchik area and the penetration to the East, between the Terek springs, occupying the town of Ordjonikidze, then the conquest of the Grozny oil centre, and finally, an attack on the Caspian Sea to Baku. For the first phase of the battle, two attack hypotheses of the 2nd Mountain Division were considered: Sajukovo-Nalchik and Baksan-Nalchik along the road between the two localities. The attack starts at the beginning of 25 October with a bombardment of the German aviation squadrons, followed by preparatory artillery blows by the mountain hunters' guns. At 8 o'clock a heavy salvo of signal throwers is fired to mark the beginning of the attack. Towards evening there is a strong Soviet counterattack with Katyusha missiles, which shows that the enemy is expecting an attack from the forces north of the river. In this bombardment Lieutenant Oltei is killed with seven soldiers preparing the materials for the passage of the 1st Mountain Pioneers Battalion. Following heavy losses, the 2nd Mountain Division was ordered to leave the conquered position, with much effort and numerous sacrifices, and to organize a defensive position on the north bank of the river. Finally, the Baksan would be forced again on 25 October, following a strong artillery and aviation training. Subsequently, the 2nd Mountain Division advanced rapidly towards Nalchik (under the command of the 3rd German Armoured Corps, commanded by Friedrich August Eberhard von Mackensen). The following day, 26 October, the Romanian troops reached the outskirts of the city on the northern edge, where the Soviet troops bravely resisted in concrete barracks and fortified buildings. Following the annihilation of enemy resistance in the cemetery on the outskirts of Nalchik, the 16th Mountain Troops Battalion conquered several blocks inside the heavily fortified city. At the same time, the 7th Mountain Troops Battalion maneuverered the town to the northeast, defeating the resistance from Salushta and Kensha, after which it attacked and conquered the houses on the west side of the city where the enemy resisted strongly. The fierceness of the fight is described as follows in the division's operations log: *"The action is progressing quite easily throughout the division, except for the city of Nalchik where strong resistance is encountered as the attackers approach the centre. Each house is in a state of defence. Through each window or wall is removed the pipe of a weapon. Large blocks and groups of houses are true centres of resistance. The streets are barricaded with obstacles against infantry and tanks, forcing the penetration of automatic weapons and anti-enemy cannons. At every crossroads or public market, there is a concrete casemate with the possibility of firing in several directions along the streets and with deep communication ditches. In the gardens of houses and parks campaign works complement those of permanent fortification. The heights*

that dominate the city on the south bank of the Nalchik brook are filled with enemy artillery and mortars"[18]. The city is surrounded, but the fighting continues the next day. On 28 October 1942, the 3rd German Armoured Corps envisaged the liquidation of all forces in the Nalchik encirclement. The 2nd Mountain Division occupied increasingly solid positions in Nalchik, including in Alexandrovskaya, and narrows the encirclement of the Soviet troops by advancing to Urban. At 7.30 a.m., after a 20-minute artillery training, the Romanian troops received the mission to conquer Nalchik, to cross the Nalchik valley and to occupy the village Casania reaching the Cerek river. Compared to the strong artillery training, the enemy's resistance was getting weaker, the targets were hit hard by both the accompanying artillery and the assault cannons, which entered the buildings and struck the defence artillery. In a raging attack, the 7th, 10th and 16th Mountain Troops Battalions conquered the city and the heights from the southeast. Defeated and disoriented, the enemy withdrew into the mountains. The city was conquered, but for the sake of victory, the fighting continued in the adjacent areas. Until 30 October 1942, the 2nd Mountain Division occupied the city of Nalchik and the surrounding area (25-28 October 1942). Here is how he addressed his subordinate troops after the defeat at Nalchik: *"I ordered you to stay a few days together, front and services, in the city of Nalchik, in front of which you bled and which you conquered with the brave soul of all. I have great joy when I see you passing serious and proud on its streets. From the zeal with which I see you running after your business, I trust that you defend with your soul, at any time, our honour, paid so dearly ..."*[19].

German Marshal Ewald von Kleist[20], the Commander of the 1st Armoured Army appreciated the victory: *"The Battle of Nalchik is one of the biggest victories of the Caucasus operations. The 2nd Mountain Division had a heroic behaviour in the battles of Vladicaucaz, when they removed from the circle a German armoured military division"*[21]. Congratulations were sent to General Eberhard von Mackensen – the Commander of the 3rd Armoured Corps and the Commander of the 4th Richtofen Air Fleet. The Battle of Nalchik ended as one of the biggest Romanian

[18] Military Archives – *Marele Stat Major* Collection - P II- 1224.
[19] According to Colonel (r) Gh. Suman, *Istoria Brigăzii 2 Vânători de Munte Sarmizegetusa,* Editura Pro-Transilvania, 2003, p. 134.
[20] Ewald von Kleist (Braunfels, Hessa, 1881 – Vladimir, 1954). German Marshal. He was, together with Guderian, the creator of the German armoured weapon. Captain of the Hussars at Tannenberg (1914), then served in the General Staff and in the Reichswehr. He led in 1940 the breakdown of the French front in Ardennes, after which he acted in the Balkans, where he conquered Thessaloniki and Athens (April 1941). He fought in Kiev (1941), Stalingrad (1942) and in front of a group of German-Romanian armies. He died in captivity in the URSS (*Grand Larousse in 10 volumes*, Volume 6: *incapacité / marbrure* ...., p. 1,758).
[21] Apud Constantin Chiper, *op. cit*., p. 11.

victories on the Eastern Front. 3,079 prisoners, a large amount of weaponry and war material were captured [22].

In the battles of Baksan and Nalchik, the Romanian 2nd Mountain Division lost 820 soldiers (157 dead, 647 wounded and 16 missing). On 2 November 1942, General Ioan Dumitrache was decorated with the Order of the *"Iron Cross"*, in the rank of Knight (Ritterkreuz des Eisernen Kreuzes), the highest Order of the Third Reich. On the same day, he received the following letter from the mayor of Nalchik:

"Dear Esteemed General,

I allow myself to express my deepest gratitude for the liberation of Nalchik on 28. X. c.

As the conqueror of Nalchik, please, in memory of this great military action, receive a gift from the city museum.

The new City Hall under my leadership will seek to bring the city and its population to well-being.

Mayor of Nalchik

Professor A. N. Dainaco"[23].

In Bucharest, on 10 November 1942, Marshal Ion Antonescu issued the Order of the Day no. 34:

"Following the fierce fighting between 25 October and 3 November, the 2nd Mountain Division, strongly supported by German air force, managed to break the enemy front on the Baksan River.

It then conquered, through close combat, numerous localities, strongly defended by Soviet troops, and entered the fortified city of Nalchik, from the foothills of the Caucasus Mountains, over which it took control by means of heavy street fighting.

Continuing the ordeal of the pursuit to *Ordjoni - kidze, the brave soldiers of this Mountain Division crushed the last attempts of resistance of the enemy, throwing his broken and disorganized remains in the mountains and capturing thousands of prisoners and a lot of war material.*

For the wonderful deeds of arms and the beautiful victory of the mountain hunters in the *"Battle of Nalchik", which will remain in the history of our great achievements, I transmit to General Dumitrache, the officers and soldiers of this glorious Division, the thanks of HIS MAJESTY THE KING and the gratitude of the MOTHERLAND, and I bow with deep respect in front of the heroes who have fallen in battle for the defeat of our enemy forever"*[24].

[22] Jipa Rotaru, Leonida Moise, Vladimir Zodian, Teofil Oroian, *Antonescu - Hitler. Caucazul și Crimeea*, Editura Paideia, București, 1999, p. 56.
[23] Military Archives, Vrancea, General Ioan Dumitrache Collection..., p. 4.
[24] *Ibidem,* p. 5.

Here are the words that General Dumitrache addressed to his soldiers, by order of the day, in those times of turmoil: *"Troops of the 2nd Mountain Division and the 10th Infantry Division: my soul is attached to your souls of martyrs of war and especially of these days. For the courage with which you arrived so well at the end of April 1944, in the name of the country you honour, I thank you with gratitude. Yet a bravery of the brave, all together, with your confidence of untroubled shooters, we will surely overcome the hard trials, defeating fate to the end, no matter how difficult it could be ..."*[25].

THE 2ND MOUNTAIN DIVISION REACHES THE EASTERNMOST POINT OF THE ENTIRE EASTERN CAMPAIGN

The offensive that followed after the conquest of the city of Nalchik is still part of the plans of the German army, the troops of the 2nd Mountain Division occupying positions on the flank of its advance. The operations begin on 2 November, with Romanian troops marching behind German armoured columns to continue the offensive towards Alagir and Ordjonikidze. *The 2nd Mountain Division reaches the easternmost point of the entire Eastern campaign, reaching about 20 kilometres from the Grozny oil centre.* Taking advantage of the fog on 14 and 15 November, the 2nd Mountain Division prepares its defensive system for winter. The enemy launches a first attack on 16 November, when it manages to enter the village of Kora-Ursdon, which it occupies. The 2nd Mountain Mounted Squadron together with the Mounted Reconnaissance Squadron try to occupy the locality, but they are rejected. Enemy reconnaissance also takes place in the other sectors of the division, but due to dense fog, such patrols are captured. In the days of the great Soviet offensive in Stalingrad, the situation on the front of the 2nd Mountain Division is a quiet one, except for an attack in the area of the 4th Mountain Troops Group given by the 37th Soviet Brigade. On days 20 and 21 only sporadic exchanges of fire are recorded. Starting from mid-November, the Romanian troops are beginning to face the adverse weather, with the presence of snow and frost, the temperatures being permanently below 0 degrees Celsius. In the slight fire exchanges with the enemy it is answered with fewer blows to save ammunition. On 24 November, at the command of the *Digora* Division, decorations are given for officers, sergeants and soldiers who distinguished themselves in the battle of Nalchik[26].

At the end of 1942, the German military command, convinced that it could no longer remain in the Caucasus, organized the withdrawal in stages starting

[25] Colonel (r) Gh. Suman, *op.cit.*, p. 163.
[26] Florin Cristescu, *op. cit.*

from the night of 31 December 1942/1 January 1943. General Auleb, by an Order of January 19, 1943 appreciated: *"The 2nd Mountain Division withdrew 200 kilometres through continuous fighting, with a spirit of sacrifice worth noting, facing the greatest difficulties under the command of its heroic and brave commander, General Ion Dumitrache"*[27].

The withdrawal was made on the route: the Taman - Crimea - Simferopol peninsula, rebuilding the troops for the military campaign of the summer of 1943. Between 13 July 1942 and 15 April 1943, the 2nd Mountain Division lost 11,000 people[28]. For his achievements, Ioan Dumitrache was advanced to the rank of Division General (1 January 1943) and received the Order *"Mihai Viteazul"*[29], class II (High Decree no. 353 of 15 February 1943), already having the same Order, class III. The Commander of the Mountain Corps, Army Corps General Gheorghe Avramescu, signed Order no. 1 519/R on 14 May 1943 to *"go to the garrison of Bucharest, being urgently called to the Carpathians, in the interest of service. Departure today 15 May 1943. Travel by plane"*[30].

On On 5 and 6 June 1943, the 2nd Mountain Division was inspected by Marshal Ion Antonescu. His appreciation paid tribute to the great mountain hunters: *"The 2nd Mountain Division was covered with glory in the Caucasus and deserves the gratitude and admiration of the country, thanks to all the staff led with honour and dignity by General Ion Dumitrache"*[31].

Between July and October 1943, the 2 Mountain Division carried out wear and tear battles with the Soviet army and partisan detachments. General Ioan Dumitrache received, starting on 24 July 1943, a leave of absence in the country for 25 days[32]. The fame enjoyed by the 2nd Mountain Division can be found in the letter

[27] Apud Constantin Chiper, *op. cit.,* p. 11.

[28] *Ibidem.*

[29] The *"Mihai Viteazul"* Order was established by the Royal Decree no. 2 968 from 26 September 1916. The initial sign of the Order was composed of a gold-plated cross, enamelled blue, with the centre on the obverse the crowned figure of King Ferdinand I, and on the reverse the year *"1916"*. Class III and Class II had the cross surmounted by the golden royal crown; in the third class - the crown had a dimension of 20 mm in length, and in the class - II - of 28 mm. The third class had a 40 mm cross and was worn on the left side of the chest; The second class, with the size of the cross of 60 mm, was worn in command and the first class, also of 60 mm, was worn as a brooch on the left side of the chest. The 1941 model had the figure of King Mihai and the year *"1941"*. The sign for the 1938 model received two crossed swords between the arms of the cross. The ribbon of the Order was of dark red-cherry mill, 37 mm wide, with on each side a 3 mm wide gold wire band. In 1936, the bearers of the Order received a kind of uniform consisting of a cloak and a cap similar to that worn by the great voivode Mihai Viteazul. It was worn by the knights of the Order on all official occasions, when the officers were required to hold the ceremony, as well as to all the national or patriotic celebrations organized by the State (Eugen Stănescu, Iulia Stănescu, Gavriil Preda, *op. cit.*, pp. 7-9).

[30] Military Archives, Vrancea, General Ioan Dumitrache Collection..., p. 6.

[31] Apud Constantin Chiper, *op. cit.,* p. 10.

[32] Military Archives, Vrancea, General Ioan Dumitrache Collection ..., p. 7.

of Marshal Ion Antonescu of 18 November 1943[33]:

During the winter of 1943, the Soviet Army decimated the warriors and combat assets of the 2nd Mountain Division. At the insistence of Marshal Ion Antonescu, the German Military Command accepted the withdrawal of troops from Crimea (11 April – 12 May 1944) by sea and by air. The units of the 2nd Mountain Division entered the peace garrisons, receiving areas of responsibility, developing intervention plans to objectives, against social disturbances, against paratroopers and partisans[34].

At the end of May 1944, the General Staff reorganized the mountain divisions into operational commands. The 2nd Mountain Division Command was transformed into the 102nd Mountain Command, being deployed, at the end of August 1944, in Deva garrison. From 1 August 1944, Ioan Dumitrache was appointed to the command of the Mountain Corps, which, from 23 August, went to annihilate the German troops in the area of Brașov.

On 31 August the troops of the Mountain Corps went on the offensive in cooperation with the 33rd Soviet Army Corps, the subordinate of which was the 1st Romanian Infantry Division *"Tudor Vladimirescu"* (established on the Soviet territory, on 2 October 1943, consisting of Romanian prisoners). On 1 September 1944, the Mountain Corps Command led by experienced General Ioan Dumitrache and the 1st Mountain Division, commanded by General Grigore Bălan, were in the border cover disposition, between Întorsura Buzăului and Homorod[35].

On 8 September, the city of Sfântu Gheorghe and, on 28 September, the city of Târgu-Mureș were liberated. By 15 October, the Mountain Corps expelled the German and Hungarian forces from the *"Intrândul Secuiesc"*. The mountain divisions liberated the cities of Sfântu Gheorghe, Baraolt, Târgu-Mureș, Aiud, Gilău, Cluj, Huedin, Beiuș, Vașcău and Oradea. Starting on 15 October 1944, the 1st Mountain Division, the Mountain Command and the corps units were withdrawn in Brașov and Sinaia, and the 2nd and 3rd Mountain Divisions continued the offensive on the territory of Hungary[36]. On 24 October 1944, Major General Ioan Dumitrache arrived in Brașov, making himself available to the General Staff. The Mountain Corps and the 1st Mountain Division were withdrawn from the combat disposition, to be disbanded based on the measures adopted by the Allied Soviet Control Commission.

On 22 November 1944, Major General Ioan Dumitrache was decorated by King Mihai (High Decree no. 2 254) with the Order *"Mihai Viteazul"* 3rd class

[33] *Ibidem*, p. 8.

[34] Constantin Chiper, *op. cit.,* pp. 10-11.

[35] Gheorghe Suman, *op. cit.,* p. 186.

[36] *Ibidem*, p. 187.

with swords *"for the way in which he distinguished himself in the heavy but successful actions during the period 24 August - 12 October 1944, undertaken in Brașov, Sfântu Gheorghe, Târgu Mureș, Gherla, for the liberation of Transylvania – Continuous in the field, in the middle of the troops, encouraging them, proving, besides personal courage, a firmness of character worthy of all the praise"*[37].

ACCUSATIONS, PERSECUTIONS, PRISON

Unjustly accused by the Soviet Military Command of committing war crimes[38], General Ioan Dumitrache was arrested. With Order no. 455 on 26 February 1945, the Military Court of Cassation and Justice, the General Prosecutor's Office ordered: *"In compliance with Order N. R. / Cabinet of the Minister / Nr. 7/1945 personally confidentially,*

I have the honour to ask you to order the immediate arrest under guard of that Command, [the Mountain Corps] of Division General Ion Dumitrache.

The officer will only be able to leave the premises only with the written approval of the Minister of War.

The record regarding this guard is attached in copy.

General Prosecutor,

General Magistrate

C. Păiș"[39].

On 7 March 1945, the Moscow Radio station transmitted the Informative Note by which General Dumitrache was accused of ordering, in October 1942, the killing of 600 prisoners, partisans, women and children at Nalchik, as well as of ordering the transport of materials to the country. The false accusations were denied by the testimony of the 127 persons who participated in the trial[40].The real reasons for his arrest were: the heroic behaviour of the soldiers of the 2nd Mountain Division in the Caucasus, for which it was nicknamed *"Divizia de Cremene"*, the refusal to continue the fighting on the territory of Hungary and the criticism of the war orders given by the Soviet commanders in *"Intrândul Secuiesc"*[41].

He was rehabilitated on 15 August 1946 and transferred to the command of the Mountain Corps, and on 1 September 1947, he was advanced to the rank of Army

[37] Military Archives, Vrancea, General Ioan Dumitrache Collection..., p. 9.
[38] The Dumitrache *Securitate* File.
[39] *Ibidem,* p. 10.
[40] Constantin Chiper, *op. cit.,* pp. 12-13.
[41] Florian Bichir, *Interogatoriul generalului Ion Dumitrache, comandant al Diviziei 2 Vânători de Munte, "Document"* - Bulletin of the Military Archives, year XIX, no. 3 (73)/2016, pp. 77-85.

Corps General and kept in reserve, having the right to receive a pension[42]. In the fall of 1948, the *Securitatea* resumed the persecutions, the general being called more frequently for interrogations.

On 3 February 1949, Ioan Dumitrache was detained at the disposal of the *Securitate* in Bucharest, being investigated between February 1949 - October 1950[43]. Without trial and conviction, he was imprisoned in Aiud and Jilava Prisons. The Prosecutor of the Bucharest Court – Instruction Cabinet – War Criminals issued, on 7 October 1950, a Certificate signed by the Chief Prosecutor: *"It is true that General in reserve DUMITRACHE IOAN was left free by us on 6 October 1950 in the matter he was preventively arrested"*[44].

He settled in Brașov, living retired, forgotten and devoid of material resources, worried about writing his memoirs. The typed text was donated to the Brașov Museum of History and Archaeology.

LETTERS OF APPRECIATION

On the occasion of the celebration of a quarter of a century since the liberation of the country and the Day of the Armed Forces, the General in reserve Ioan Dumitrache received, on 5 March 1970, an exciting and respectful letter from Ștefan Pașcanu, from Târgu Mureș[45]:

"Dear General Dumitrache,

The quarter of a century that passed made us remember and tell the deeds of arms carried out to defend the homeland. In order to be better documented, your precious help was requested, for which we ask you to receive the warmest and most sincere thanks.

We have no words to appreciate the extraordinary content of the file, including the military operations carried out by the brave Mountain Troops under your skill, command and strategy.

Remarkable and true pearls of literature and authentic patriotism are the orders of the day issued by you. after the glorious battles waged in the Mureș area, along the thousand-year-old Ardeal.

We started holding a series of presentations on this topic related to the anniversary of the Liberation of the homeland and the anniversary of our Armed

[42] *Ibidem,* p. 13.
[43] *Ibidem.*
[44] Military Archives, Vrancea, General Ioan Dumitrache Collection..., p. 11.
[45] Horia Dumitrescu, Marilena Sima, *Generalul de corp de armată Ioan Dumitrache (1889 - 1977). Contribuții, "Cronica Vrancei"* XIX, Vrance Museum, 2014, pp. 369-393.

Forces, among which a large meeting you were invited to attend and to make a speech.

Regardless of our will, the great meeting did not take place and we learned that you were kind enough to come to our city.

It is good. The land of the country knows our steps. The word country is encrusted with living flesh. It is our saints who have fallen for it.

It would be true and just that the survivors of the bloody days should pay more attention, with more gratitude, not so much to our person as to the valuable contribution we can bring to the patriotic education of the youth in propagating the love of the ancient soil, in the fight against the forgetfulness of the fierce clashes with the enemy, of the great blood tribute paid for the difficult today and the happier tomorrow of our homeland and our people.

Dear General,

In the evocations related to the 25th anniversary of the Liberation and the anniversary of our Armed Forces, in our exhibitions, we honour and we will always do so the name, the luminous figure of the strategist, of the great patriot, of the man, General Ion Dumitrache.

Returning your precious material, we thank you wholeheartedly for your kindness in making it available to us. It will be the most valuable piece, the most expensive material for our work not always carried out in the best conditions and, in some cases, maybe not understood properly.

Please receive our homage and warmest and sincere wishes for you to be fine and healthy for many years in the future.

Best regards to your Lady

Yours sincerely,

War veteran. Antifascist"[46].

The survivors of the 1916 promotion B active and reserve infantry and administration officers met on Sunday, 28 May 1972, in the former premises of the Military Infantry and Administration School in Bucharest, to celebrate the 55th anniversary since the first officer degree was obtained. The 40 participants sent him a letter, signed by all, expressing their homage to the one who led them in the battle and was a model of their conduct and virtues in life:

"Well respected General,

The survivors of the 1916 Promotion B, active and reserve infantry and administration officers, assembled today in the former Military Infantry

[46] *Ibidem*, pp. 12-13.

and Administration School in Bucharest to celebrate the 55th anniversary since their promotion to the first officer rank, with the sincere and deepest regret that – because of reasons exceeding our desire and possibilities – we could not have you among us, in this festive and dear to us circumstance, we send you a warm and respectful greeting and assure you of the most pleasant memories of life and our sincere gratitude, for all that you have given us, as a gift, from your mind and soul, for the most perfect and thorough formation of us for life and for the noble and beautiful career of apostolate and sacrifice, which we embraced with affection and fulfilled with honour. -

We all wish you, with all our heart, that fate will continue to reserve many happy returns of your venerable age!"[47].

He died on 6 March 1977, being buried in the Groaveri Cemetery in Brașov. Today, in Brașov, two small neighbouring streets bear the names of generals Dumitrache and Mociulschi, two great personalities of the Romanian Army.

Among those who expressed condolences were Gheorghe Mihail[48*]. On a business card, General Mihail wrote:

"Army General Gh. Mihail

Former Supreme Commander of the Armed Forces

Former Chief of the Armed Forces Great General Staff

I express sincere condolences for the death of my dear comrade General Dumitrache, a brave general, who helped me in the heavy responsibility I had on 23 August 1944.

Versailles – France

22 March 1977"[49].

[47] *Ibidem,* pp. 14-15 verso.

[48] *Gheorghe Mihail (13 March 1887 – 2 February 1982). Second Lieutenant (1907), Major (1917), Brigadier General (1935), Adjutant Division General (1939). Commander of the Special Infantry School (1929 - 1930), Chief of Staff of the General Inspectorate of the Army (1936 - 1937), Chief of the General Staff (August - September 1940, August - September 1944), Inspector General of the Infantry (1944 - 1945) and the Army (1945 - 1947), Undersecretary of State at the Ministry of National Defence in the government of Constantin Argetoianu (28 September - 23 November 1939), Vice-President of the Council of Ministers (4 July - 24 August 1940). He participated in the First World War, being wounded in the Battle of Mărăşeşti. On 23 August 1944 he was appointed Chief of the General Staff. He coordinated the operations to cover the frontiers, to liquidate the German armed forces and to disarm the large units of the Wehrmacht in Romania (23 - 31 August 1944). See C. Căzănişteanu, V. Zodian, A. Pandea, *Comandanți militari. Dicționar*, Editura Științifică și Enciclopedică, București, 1983, p. 220.

[49] Military Archives, Vrancea, General Ioan Dumitrache Collection..., p. 16.

INSTEAD OF CONCLUSIONS: MOUNTAIN TROOPS DAY – 2 NOVEMBER 1991, BRAŞOV

The celebration of the Mountain Troops Day, on the 75th anniversary since the establishment of the first units [50], took place at the Military Circle in Brașov, on 2 November 1991.

The program included the Symposium with the theme fighting traditions of the mountain troops of the Romanian army, the premiere presentation of the films *Vânătorii de munte/Mountain Troops* – brief history and *Manevra/Manoeuvre*, the unveiling of the triptych where the Mountain Troops monument was to be located. After the Symposium, during a festive event, there were handed the commemorative plaques, badges and diplomas *"75 de ani de la înființarea vânătorilor de munte în armata română"*/ 75 years since the establishment of the Mountain Troops in the Romanian Armed Forces[51].

Invited to these events, Mrs. Aurica Dumitrache received a Diploma awarded to the post-mortem general Colonel Ion Dumitrache for his entire military career[52]:

General Ioan Dumitrache remains one of the most perennial and illustrative military personalities with whom the Romanian Armed Forces has pervaded History.

BIBLIOGRAPHY

1. ***, National Council for the Study of the *Securitate* Archive, *Criminal Collection*.
2. ***, National Military Archives of Romania, *Marele Stat Major Collection*.
3. ***, Mountain Troops Archives, *General Ioan Dumitrache Collection*.
4. ***, *Grand Larousse en 10 volumes,* Librairie Larousse, Paris, 1993, vol. 9.
5. Valeriu Anghel, Alexandru Deşliu, *Vocaţie* şi *destin. 600 fişe-portret pentru un tablou spiritual-istoric al judeţului Vrancea*, Editura Terra, Focşani, 2000.
6. Florian Bichir, *Interogatoriul generalului Ioan Dumitrache, comandant al Diviziei 2 Vânători de Munte*, in *"Document", Buletinul Arhivelor Militare*, year XIX, no. 3 (73)/ 2016.
7. C. Căzănişteanu, V. Zodian, A. Pandea, *Comandanţi militari. Dicţionar*, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1983.
8. Constantin Chiper, *General de corp de armată Ioan Dumitrache*, in *Veterani* în *slujba Patriei*, vol. II, under the aegis of the National Association *"Cultul Eroilor"*, Editura BURATINO, Ploieşti, 2006.

[50] According to the Order of the Great Headquarters no. 294/3 November 1916, the School of Skiers - established on 30 September 1916 in the barracks of the 4th Regiment Roşiori in Bucharest, with a staff of 1,000 soldiers - was transformed into the Mountain Troops Corps, a fighting unit organized by three battalions, totaling 1,980 soldiers. At the command of this unit was named captain Virgil Bădulescu (Gheorghe Suman, *op. cit.,* p. 179).

[51] Military Archives, Vrancea, General Ioan Dumitrache Collection …, pp. 17-18.

[52] *Ibidem*, p. 19.

9. Florin Cristescu, *Operaţiunile Diviziei 2 Munte* în *Munţii Caucaz,* http://www.historia.ro/exclusiv_web/general/articol/opera-iunile-diviziei-2-munte-n-mun-ii-caucaz
10. Horia Dumitrescu, Marilena Sima, *Generalul de corp de armată Ioan Dumitrache (1889-1977). Contribuţii*, *"Cronica Vrancei"*, XIX, Vrancea Museum, 2014.
11. Adrian Pandea, Eftimie Ardeleanu, *Românii în Crimeea. 1941-1944,* Bucureşti, 1995.
12. Florian Răpan, Dorel Buşe, *Învăţământul militar,* in *Enciclopedia Armatei Române,* Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009.
13. Jipa Rotaru, Leonida Moise, Vladimir Zodian, Teofil Oroian, *Antonescu - Hitler. Caucazul* şi *Crimeea*, Editura Paideia, Bucureşti, 1999.
14. Eugen Stănescu, Iulia Stănescu, Gavriil Preda, *Cavaleri ai Ordinului "Mihai Viteazul*", Editura UNIVERSAL CARTFIL, Ploieşti, 1996.
15. Gheorghe Suman, *Vânători de Munte* in *Enciclopedia Armatei României*, Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009.

Președintele României

Dorind a răsplăti meritele

revistei

„Gândirea militară românească"

cu ocazia împlinirii a 110 de ani de existență, pentru rezultatele de excepție obținute în implementarea doctrinei a construcției militare naționale și pentru contribuția fundamentală adusă la edificarea concepțiilor strategice care au susținut transformarea profundă a Armatei României la nivelul standardelor operaționale ale Alianței Nord-Atlantice,

Conferă Ordinul „Meritul Cultural"

în gradul de Cavaler categoria F „Promovarea culturii"

Dat în București la 24-08-2004

Președintele României

Ministrul Culturii și Cultelor — Ion Iliescu — Cancelarul Ordinelor

Decret nr. 646 Din 24-08-2004

Brevet MC/I nr. Cult, F, 2 Nr. crt. 76755

Order *"Meritul Cultural"* in the rank of *"Knight"*, F Category – *"Promotion of Culture"* (Presidential Decree no. 646 on 24.08.2004)

Președintele României

Dorind a răsplăti meritele

Revistei

Gândirea Militară Românească

în semn de recunoaștere a contribuției fundamentale la edificarea conceptelor strategice care au susținut construcția militară națională și transformarea profundă a Armatei României,

Conferă

Ordinul „Meritul Cultural" în grad de „Ofițer", Categoria F - „Promovarea culturii".

Președintele României

Ministrul — Traian Băsescu — Cancelarul Ordinelor

Decret nr. 483 din 30.06.2014

Brevet MC 04 Ian. 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