ROMANIAN MILITARY THINKING

FOUNDED IN 1864 UNDER THE NAME "ROMÂNIA MILITARĂ"
- NEW SERIES, YEAR XVI -

3/2020

JOURNAL OF MILITARY SCIENCE AND SECURITY STUDIES PUBLISHED BY THE DEFENCE STAFF

EDITORIAL OFFICE
București, 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

Printed
at Military Technical Publishing Centre
C ___/2020 B ____

PUBLISHER
THE DEFENCE STAFF

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 oficers, belonging to all branches, who are in active duty, will be able to publish their personal papers and the ones that interest the Armed Forces".

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

ROMANIAN MILITARY THINKING

Journal of Military Science and Security Studies Published by the Defence Staff

Founded in 1864 under the name *"România Militară"*
– new series, year XVI –

ISSN Print: 1841-4451
ISSN Online: 1842-824X
Romanian Military Thinking is a scientific journal with acknowledged prestige in the field of "*Military Science, Intelligence and Public Order"*, in keeping with the evaluation carried out by the National Council for Titles, Diplomas and Certificates (CNATDCU) in 2011 (http://www.cnatdcu.ro/wp-content/uploads/2011/11/reviste-militare1.pdf)

Romanian Military Thinking Journal is included in the Journal Master List of the **INDEX COPERNICUS INTERNATIONAL and EBSCO's ,** International Security & Counter-Terrorism Reference Center databases, **and ROAD Catalogue**

A LEGACY SINCE 1864

The Romanian Armed Forces road to modernity started in 1859, once the United Principalities General Staff Corps, currently the Defence Staff, was established.

Soon after it, in 1864, a group of nine captains, graduates of the first series of the Officer Cadet School in Bucharest, took the initiative to develop a *"military science, art and history journal"* named *"România Militară/Military Romania"*.

The initiators of the publication – **G. Slăniceanu** (Captain, Chief of the Engineer Battalion), **A. Gramont** (Staff Captain), **G. Borănescu** (Engineer Captain), **G. Anghelescu** (Staff Captain), **A. Anghelescu** (Artillery Captain), **E. Arion** (Artillery Captain), **E. Boteanu** (Staff Captain), **E. Pencovici** (Staff Captain) and **C. Barozzi** (Engineer Captain) –, educated not only in Romania but also abroad, were inspired by the necessity to develop a substantial theoretical activity in the Romanian Army too.

The journal manifesto[1], included in the first issue, which appeared on 15 February 1864, contained innovative ideas and approaches that were meant to:

"- contribute to the organisation of our military system the Legislative Chamber is about to decide upon soon;

- assemble and examine the Country old military institutions that had made for the glory of Romania for several centuries and ensured our existence;

- explore, in the absence of any military study, all the aspects related to the Army training, the most solid basis of the armed forces;

- get the Romanian Troops well-informed about the military events in the world;

- join efforts to work concertedly and whole-heartedly to develop and strengthen the edifice that is meant to ensure the future of our country"[2].

"România Militară" was an independent publication, under the aegis of the War Ministry, and it ceased to appear in 1866 as there were no sufficient funds and subscribers. The publication was resumed in 1891, about a quarter of a century later, also as the result of the initiative of a group of officers in the Great General Staff who intended to *"reproduce the serious studies on the organisation, strategy and art of commanding troops under any circumstances"*[3]. Shortly after it, by the Royal Decree no. 3663 issued on 8 December 1897, *"România Militară"* became the *"Great General Staff official publication"*.

C. Barozzi
(Engineer Captain)

E. Pencovici
(Staff Captain)

E. Boteanu
(Staff Captain)

G. Borănescu
(Engineer Captain)

G. Anghelescu
(Staff Captain)

G. Slăniceanu
(Captain, Chief of the Engineer Battalion)

E. Arion
(Artillery Captain)

A. Anghelescu
(Artillery Captain)

[1] *Din trecutul României Militare cu prilejul aniversării a 75 de ani de la apariția ei în viața armatei. 1864-1939*, București, 1939, p. 31.
[2] *Ibidem*, p. 32.
[3] *România Militară*, no. 1, 1981, p. 6.

English version by **Diana Cristiana LUPU**.

The *GÂNDIREA MILITARĂ ROMÂNEASCĂ*
Journal Awards
are yearly bestowed,
by the Romanian Armed Forces Defence Staff,
on the most valuable works in the field
of military science, published in the previous year

"Brigadier General Constantin Hîrjeu" Award

"Lieutenant Colonel Mircea Tomescu" Award

"Division General Ștefan Fălcoianu" Award

"Army Corps General Ioan Sichitiu" Award

"Marshal Alexandru Averescu" Award

CONTENTS

SOCIETY RESILIENCE IN THE CONTEXT OF THE COVID-19 PANDEMIC AND THE ARMED FORCES ROLE IN THIS PROCESS

Major General Gheorghiță VLAD

Deputy Chief of Defence Staff for Operations and Training

The world has been facing, since the beginning of 2020, a medical crisis – a pandemic that could be classified in the category of known knowns – known dangers. Human history has recorded such situations before. They are known to us because they have been immortalised through art, literature or films – from both historical and futuristic-dystopian perspectives. There have also been warnings over time, from international organisations in the healthcare field, about such a health security risk. However, the pandemic generated by the coronavirus SARS-CoV-2, which causes COVID-19 disease, is the security scenario for which humanity, in general, has been very poorly prepared.

Framing a pandemic as a security issue means neither "it's time to panic" nor a pandemic should be equated with a war or a military problem. However, it is certainly a security issue. Therefore, managing the situation requires lucid minds and the best possible information, often when data are incomplete or insufficient. This type of crisis illustrates

the complex nature of security, in which several actors are involved, and good civil-military cooperation is essential for understanding the big picture. The COVID-19 pandemic is not one of the challenges that is commonly seen in militarised security (the use of force), but it has shown us that it could, however, destabilise entire societies. Therefore, it is not a big surprise that when things got really complicated, the armed forces were involved. This is not an event that is unprecedented. Whenever a natural or man-made disaster occurs, the armed forces become one of the basic solutions for governments in generating their response. Most countries have legislation in place that allows for the use of armed forces to support civilian authorities in crisis situations and non-military emergencies.

The Romanian armed forces supported the central and local authorities by installing three ROL 2 hospitals in Bucharest, Constanța and Timișoara, by installing over 50 epidemiological triage units in military and civilian hospitals in the country, by performing approximately 25,000 tests to detect COVID-19, by ensuring the temporary management of three county hospitals in Suceava, Deva and Focșani. Moreover, the military participated, during the state of emergency, in about 100,000 missions, being near the people in difficulty, distributing about 4,000 packages containing food and hygiene products to war veterans and widows in 10 counties. The military personnel in the Romanian Air Force conducted over 20 missions through which they ensured the air transport of approximately 270 tons of medical protection equipment, as well as the evacuation of some Romanian citizens from abroad. Military researchers managed to execute, in record time, a transport isolette, which was homologated and entered series production, as well as a technological demonstrator for a mechanical ventilator, two products extremely useful to the medical system. Last but not least, because, in such moments, there is a need, more than ever, for solidarity, compassion and unity, military specialists and medical staff have been co-opted into the teams deployed to support the efforts of the Moldovan and the US authorities to manage the pandemic.

Therefore, when faced with critical deficiencies in the capabilities of civilian institutions during a major disaster, governments naturally

turn to military capabilities. Why the military personnel can manage a crisis situation more efficiently is a question that can be answered by providing some reasons that underlie the existence and functioning of the military system.

First of all, strong leadership is essential. The transition to war conditions requires leaders who are constantly prepared for it, not decision-makers who deny reality. As organisations, military systems are uniquely configured to deal with the harshest war conditions, war being a situation that tests, stresses and extends the limits of all human faculties – physical, psychical and mental. It includes a range of capacities and capabilities that very few other organisations implement – from command and control to logistics and resource management, from healthcare and CBRN protection to transportation and engineering, from intelligence and surveillance to strategic communications and even internal research and development and so on.

Secondly, information makes the difference. Although not always complete or fully accurate, information underpins all military decisions. Navigating the "fog of war" is impossible without information. Many authorities ignored the pandemic early warning signals, and some governments failed to make the necessary efforts to have a complete picture of the spread of the infection within their borders.

Thirdly, the military personnel are trained to consider time a critical resource that cannot be recovered when it is lost. Under such conditions, availability entails permanent and rigorous planning, which constantly adjusts the courses of action and the allocation of resources, because a dynamic situation evolves rapidly and uncertainty increases exponentially. Therefore, the reaction speed and a proactive approach matter a lot. Once the spread of the pandemic generated an exponential increase in many countries, the authorities were constantly behind the curve, wasting precious time as a result of the implementation of half measures, thus having to react rather than model events.

In another train of thoughts, for the military, "logistics is the component that ensures success in combat". Some observers have compared the situation of under-resourced doctors to sending military troops into battle without weapons and protective equipment. The military personnel are

educated in the management of war logistics and have the advantage of learning much from military history and, not infrequently, from their own experience. Moreover, in the military mindset, reserve stocks are very important. The military personnel know that they must have reserves for absolutely anything, because losses will inevitably occur and will have to be replaced quickly.

Last but not least, mental training and morale are aspects that are strongly emphasised. Through a variety of techniques and practices, military structures aim to maintain the cohesion of units and the morale of individuals under the spectrum of warfare. These techniques can, in some cases, be replicated in society during crisis situations, such as the ongoing pandemic. An example in this regard is the principle that "no one is left behind", which underlies the morale of the military personnel in battle. Many governments and societies have embraced this technique in the face of the coronavirus pandemic – no one has been left without support following the border closures, the elderly have not been abandoned in self-isolation, teams of volunteers have distributed food to those in need etc. It was an extremely strong message, which contributed to the management of the pandemic, so that its effect could be as limited as possible.

The conclusion is that military organisations and their members internalise many elements of resilience in extreme situations as part of their work and lives, and can therefore inspire, guide and support parent societies in times of need if asked for support. Yet, as the military personnel are well aware of, the road to resilience begins long before war hostilities break out and it is often based on the ability to keep a healthy focus on worst scenarios, even when times are relaxed and peaceful. It is clear from the current pandemic that in order to manage crises we need to think critically about the role of comprehensive approaches involving multiple actors, starting from governments, civil society, the private sector, the military and the police, and last but not least, the citizens and their communities.

INFORMATION WARFARE/OPERATIONS OF THE RUSSIAN FEDERATION IN THE CONTEXT OF *SARS-COV-2*

Major Petre SCÎRLET
"Carol I" National Defense University, Bucharest

Lecturer Cristian ICHIMESCU, PhD
"Carol I" National Defense University, Bucharest

High-impact global events, such as the Covid-19 pandemic, occur very rarely – probably several times over a century – and produce, among other things, major geopolitical changes, targeting alliances, political blocs, regions, states and areas of influence.

The Covid-19 pandemic quickly affected the entire world, and the personal freedom of billions of people was restricted in an unprecedented way. However, the pandemic has not frozen the conflicts between various states of the world.

Although a global response to the SARS-CoV-2 coronavirus crisis is needed, the Russian Federation does not consider it in its best interest to contribute – and, in fact, the Kremlin is using the crisis to further destabilise the world.

Thus, simultaneously with the virus, an enormous amount of data and information is spreading all over the world, many of them being part of a large campaign to influence public opinion through warfare/information operations planned and executed by the Russian authorities.

The global framework created by the expansion of the pandemic represented the operational moment identified by the Kremlin to implement, once again, the complex machinery represented by information warfare/operations, which have thus become the most complex form of modern confrontation.

Keywords: information activities, Covid-19, disinformation, infodemia, cyber operations

WHAT IS/ARE CONTEMPORARY INFORMATION WARFARE/OPERATIONS?

The Romanian Doctrine from 2017, SMG-66, named the *Doctrine for Information Operations*, defines the notion of information operations as representing "*a staff function intended for the analysis, planning, evaluation and integration of all information activities in order to obtain the desired effects on the will, understanding, perception and capabilities of adversaries, potential adversaries and target audiences, approved by the CSAT* [Supreme Council of National Defence – editor's note]*, in support of the achievement of military objectives*"[1].

In 2009, NATO, within the doctrine AJP-3.10, *Allied Joint Doctrine for Information Operations*, defined *information operations* as being "*a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives*"[2].

NATO, within the doctrine AJP-3.10, Allied Joint Doctrine for Information Operations, defined information operations as being "a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives".

Analysing the definitions presented above, we can notice a series of similarities. According to the two doctrines, information operations are identified by the *effects* produced on three distinct categories: will; understanding and perception; capabilities. In addition to studying the doctrines mentioned above[3], information operations are put into practice by performing certain types of activities, namely influencing activities, activities against control and command capabilities, and activities of information protection.

According to some authors, for the Russian Federation, the concept of information warfare implies "*computer network operations alongside disciplines such as psychological operations, strategic*

[1] S.M.G.-66, *Doctrina operațiilor informaționale,* București, 2017, p. 15.
[2] AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009, pp. 1-3.
[3] AJP-3.10, *op. cit.*, p. 1-7, and S.M.G.-66, *op. cit.*, p. 21.

communications, influence"[4] and "*intelligence, counterintelligence, maskirovka, disinformation, electronic warfare*"[5].

We can thus notice the difference between the two meanings (NATO/Romania vs. the Russian Federation) in the sense of the complexity of the concept approached by the Kremlin, which is an extended concept and covers a wide and diverse range of activities. Thus, we notice that, for the Russian Federation, all areas form a unit under the concept of *information warfare* while NATO approaches the concept of *information operations*. Throughout this article, we will use the concept of information warfare/operations to characterise the information actions of the Russian Federation.

Throughout the Cold War, the Soviet strategy resorted to a series of so-called "active measures", which describe actions and strategies designed to influence the decisions of a state, its population and important political, military and social events in that state.

A characteristic of the information warfare/operations carried out by the Russian Federation is the offensive character, which has been found in all the information campaigns carried out by this state over time against various state actors. We will further present a short history of information warfare/operations implemented by the Russian Federation through the use of important areas, such as disinformation and active measures.

RUSSIAN HISTORY OF INFORMATION WARFARE/OPERATIONS

The basic ideas on which some of the forms of information warfare/operations carried out by the Russian Federation is/are based are not new, their origins dating as early as the Cold War. Throughout the Cold War, the Soviet strategy resorted to a series of so-called "*active measures*", which describe actions and strategies designed to influence the decisions of a state, its population and important political, military and social events in that state.

Allegations that the United States carried out biological weapons attacks were common accusations by opponents such as the USSR or Cuba, which sought to accredit to the international community the idea that the United States had violated the Biological Weapons Convention.

[4] Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, p. 7.

[5] Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 March 2011, http://www.rferl.org/articleprintview/2345202.html apud Keir Giles, *op. cit.*, p. 7.

While many allegations of biological weapons originated in the Kremlin, those were often amplified by media sources in the USSR's allied states. The Cuban media consistently claimed that the United States spread a variety of diseases in the period 1970-1980. At the same time, Russian authorities accused the United States of involvement in the development of particularly dangerous mosquito species in Pakistan, to be used for the rapid spread of biological weapons[6].

The accusations against the United States regarding the use of biological weapons were a practice often used by opponents during the Cold War, but the two most insidious campaigns were those related to the Korean War[7] and the AIDS disinformation campaign[8].

It can be seen that, during the Cold War, taking the NATO definition of information operations as a theoretical basis, the USSR mainly used *information activities to create the desired effects on the understanding and capabilities of different audiences*. We also observe the planning and execution, in particular, of influencing activities and information protection activities.

During the Cold War, taking the NATO definition of information operations as a theoretical basis, the USSR mainly used information activities to create the desired effects on the understanding and capabilities of different audiences.

Accusations of biological weapons surrounding the current SARS-CoV-2 pandemic continue the specific line of information warfare/operations conducted by the Soviet Union during the Cold War, but the confrontational capabilities and objectives pursued are much more complex.

The Russian Federation is currently leading perhaps one of the largest and most complex information warfare in recent years, integrating sequences of media operations, manipulation, disinformation, propaganda – white, black and gray, social media operations, cyber operations and involving the whole arsenal of tools specific to the information warfare, among which we would mention

[6] Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, Vol. 57:205-227 (Volume publication date January 2012), https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618 retrieved on 11 April 2020.

[7] For further information, Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 April 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/

[8] For further information, Douglas Selvage, Christopher Nehring, *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*, 22 July 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids and Filippa Lentzos, *The Russian Disinformation Attack that Poses a Biological Danger*, 19 November 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/

the accusation of the opponent for committing atrocities, propaganda or discrediting the opponent's propaganda, exaggerated amplification of certain stakes, invoking protection etc.

All the confrontation capabilities listed above are used, but the dimension of disinformation along with the cybernetic one stands out from the other forms.

THE CORONAVIRUS OF DISINFORMATION – THE NEW RUSSIAN INFORMATION WARFARE –

During this period, a large number of people are locked in their houses and spend a lot of time on social media. According to the data, at the end of March, there were more than 3 billion posts and over 100 billion interactions on *#covid19*, *#coronavirus* and the like[9].

As early as 2 February this year, the World Health Organization (WHO) warned that the world was facing two epidemics[10] in parallel: one caused by the new coronavirus SARS CoV-2 and a second referring to a so-called "*infodemia*", describing this phenomenon as an overabundance of more or less accurate news.

The narrative proposed by the vectors of the Russian Federation mainly aims at altering the public space of the targeted audiences by injecting disinformation and propaganda. At the same time, another pillar is that of the lobby, which aims to influence the target audience through ideas conveyed in the public space by legitimate and credible message bearers.

Last but not least, elaborate psychological operations are used where the information disseminated but especially its effect on the target audience, namely the birth and creation or accentuation of fears, collective emotions, the preparation of the public to react to future events in a directed formula.

The narratives of the Russian Federation

Russian narratives can be divided into three categories: a so-called basic disinformation; complex disinformation and elaborate propaganda.

[9] Faruk Zorlu, *Covid-19: Infodemic Spreads Faster than Pandemic*, 31.03.2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381 retrieved on 13 April 2020.

[10] The WHO raised the level of the Covid-19 epidemic to the level of a pandemic on 11.03.2020.

ROMANIAN MILITARY THINKING

Basic disinformation consists of the least sophisticated types of disinformation. These approaches target the least informed public of the Russian masses and beyond, among whom the anti-American sentiment is historically strong and easily inflamed. The tools used include disinformation platforms, bloggers, as well as accounts used by Russians living in the US, Canada and the EU. For this target audience, Russian propagandists deliberately use unsophisticated language and primitive but convincing, simple arguments[11].

Complex disinformation promulgates similar ideas, but dressed differently. This approach is based on elaborate conspiracy theories that aim to create the so-called alternative reality and try to promote mistrust among the foreign public. Russian news platforms use pseudo-scientific "*evidence*" that the virus was created in an American laboratory to stop China's economic growth[12].

The third category presents an example of *elaborate propaganda*, designed for very narrow circles outside the Russian Federation. In this case, the Russian state relies on its own prominent scientists and sometimes uses foreign sources (mainly Chinese). According to their theories, "*Coronavirus ...has become the end of the modern world"*[13]. It is claimed that the world order established after the Cold War is now collapsing and giving way to a new period in which new leaders will emerge.

"*Disinformation plays with people's lives. Disinformation can kill*" said Josep Borrell, director of the European External Action Service, at a news conference in the second decade of March. This dangerous game started at the beginning of this year and has developed gradually.

The first disinformation on Covid-19 appeared in *Sputnik News* on 22 January[14], when an article was published stating that the virus was man-made, being a weapon created by NATO[15].

Complex disinformation promulgates similar ideas, but dressed differently. This approach is based on elaborate conspiracy theories that aim to create the so-called alternative reality and try to promote mistrust among the foreign public.

[11] *NATO Uses COVID-19 to Mobilise Western Military Forces against Russia*, 19.03.2020, interview with Alexander Artamonov for Novorossia News Agency, https://novorosinform.org/808651 retrieved on 13 April 2020.

[12] Vicky Peláez, *Scientists: Coronavirus Would Be a Weapon of Biological Warfare*, 13.02.2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/ retrieved on 14 April 2020.

[13] Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 05.04.2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship retrieved on 14 April 2020.

[14] *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/ retrieved on 14 April 2020.

[15] *A New Chinese Coronavirus Was Likely Elaborated in NATO Biolabs*, https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/, retrieved on 14 April 2020.

According to a study conducted by EUvsDisinf[16], analysing articles published in foreign media between 22 January and 25 March on the topic of Covid-19, the favourite target remains the USA, with 39 articles, articles in which it is claimed that the USA created the SARS-CoV-2 virus. The second most common narrative, with 26 published articles, is that the EU is failing to cope with the crisis and is disintegrating as a result, along with the Schengen area. In particular, this narrative of the EU's failure and lack of solidarity is on trend following the delivery of Russian aid to Italy. The narrative that the virus is used as a weapon against China and its economy comes third with 24 articles. The narrative that the entire coronavirus crisis is a secret plan of the global elite lies fourth, with 17 articles[17].

In the military, the disinformation targeted the multinational exercise Defender Europe 2020. The Russian leadership criticised the exercise as an offensive "anti-Russian scenario", but then used propaganda to spread the theory that executing the exercise could facilitate the spread of the SARS-CoV-2 virus in Europe due to the arrival and movement of a large number of troops.

In the military, the disinformation targeted the multinational exercise *Defender Europe 2020*. The Russian leadership criticised the exercise as an offensive[18] "*anti-Russian scenario*", but then used propaganda to spread the theory that executing the exercise could facilitate the spread of the SARS-CoV-2 virus in Europe due to the arrival and movement of a large number of troops.

Channels used

To achieve its goals, Moscow has a number of message propagation vectors that can be divided as follows:

1. Traditional media (*Russia Today* trust, which also owns Russia Today television station and *Sputnik* project*, Pervy Kanal*);
2. The virtual environment (the Kremlin's troll army) – structures specialising in activities on blogging platforms, news production, creating images and denigrating content to undermine a certain target, producing video content and writing pro-Kremlin comments posted in virtual environments. According to a report prepared for the Global Engagement Center[19] within the US State Department, the use of accounts controlled by the Russian state was noticed, initially used to influence the specific events of the conflict in Syria and the extensive strikes in France, to post messages related to the coronavirus pandemic.

   According to the Department of State, when the Russian media began broadcasting anti-Western articles and interviews about the origins of the SARS-CoV-2 virus, Russian accounts started to promote them worldwide, covering more than 20 languages – from English to Russian and from Serbian to Arabic.
3. Involvement of influential figures from the Russian Federation, opinion formers enslaved to the Kremlin. Obviously, this picture could not miss one of the most influential geopolitical thinkers of the Russian Federation, Alexander Dughin, a Russian nationalist and a very public supporter of the Orthodox Church, who claimed that when the virus ends its march of victory across the planet, the existing world order will be destroyed. It is well known that its messages are part of the Russian agenda, intensely promoted in recent years, being one of the main tools through which Russian propaganda builds, promotes and develops the constituent elements of a brand image of the Russian Federation.
4. NGOs, think tanks and other discussion platforms whose purpose is to disseminate Russian propaganda.
5. And last but not least, we mentioned the involvement of Russian intelligence services in promoting messages in support of Russian foreign policy at EU level. They use freelance journalists, journalists, NGOs and research institutes.

According to a report prepared for the Global Engagement Center within the US State Department, the use of accounts controlled by the Russian state was noticed, initially used to influence the specific events of the conflict in Syria and the extensive strikes in France, to post messages related to the coronavirus pandemic.

If over the US the information warfare of the Russian Federation are aimed at destabilising and discrediting the US at the European level, taking advantage of the United States' inability to help its allies, the agenda for the European Union is more complex, aiming to undermine cohesion by cultivating a concentration of information activities on some EU member states.

[16] *EUvsDisinfo* within the East StratCom Task Force is the project of the European External Action Service. It was set up in 2015 to respond to the Russian Federation's disinformation campaigns affecting the European Union. For more information https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

[17] *Ibid.*

[18] *The US Defender 2020 Military Manoeuvre Is Explicitly Directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia after Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen*, https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title retrieved on 14 April 2020.

[19] Lea Gabrielle, *Briefing on Disinformation and Propaganda Related to COVID-19*, https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19 retrieved on 14 April 2020.

In this context, Moscow emulated China's movements to send aid to Italy and Spain and acted to claim all publicity and benefits.

From Russia, with love...

Moscow's aid to Italy in connection with the coronavirus has been widely covered in both the international[20] and Russian press. Italy gratefully welcomed the arrival of a Chinese plane – in the presence of the Italian president and the Chinese ambassador – carrying doctors and equipment.

The Russian state media presented the situation in Italy in the context of the country's struggle to limit the spread of coronavirus in different ways.

On Radio Vesti FM, controlled by the Kremlin, the public was told that the coronavirus epidemic would force Italy to leave the EU. Earlier, the Kremlin-controlled Sputnik promoted the conspiracy theory that the coronavirus could have been created to limit the economic burden of retired citizens on Italy's budget.

On *Radio Vesti FM*, controlled by the Kremlin, the public was told that the coronavirus epidemic would force Italy to leave the EU[21].

Earlier, the Kremlin-controlled *Sputnik* promoted the conspiracy theory that the coronavirus could have been created to limit the economic burden of retired citizens on Italy's budget[22].

Sputnik also accused members of the European Parliament of wanting to launch a campaign against Russian aid to Italy, when in reality they asked to analyse disinformation campaigns and the geopolitical use of aid.

At the same time, a video was intensely promoted in the Russian media in which an Italian citizen replaced the flag of the European Union with that of Russia, falsely conveying the idea that this current is a widespread one. A BBC television reporter contacted the Italian citizen to request a point of view stating that he had decided to raise several Russian Federation flags outside the store he owns to express his gratitude to Russia.

Another video that was distributed in the pro-Kremlin press shows the anthem of the Russian Federation being sung in Italy. Among the Russian publications that broadcast the video were the state-controlled network *Rossiya 1* and the pro-Kremlin television channel *REN TV*,

[20] According to an analysis by the Italian daily La Stampa, about 80% of the supplies sent by Russia are "*useless*" according to Jacopo Iacoboni, La Stampa, 25.03.2020, *Coronavirus, la telefonata Conte-Putin agita il governo: "Più che aiuti arrivano militari russi in Italia",* https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327 retrieved on 15 April 2020.

[21] *Coronavirus: BBC Challenges Pro-Kremlin Reporting from Italy,* 01.04.2020, https://euvsdisinfo.eu/coronavirus-bbc-challenges-pro-kremlin-reporting-from-italy/ retrieved on 15 April 2020.

[22] *Ibid*.

whose story was presented online under the headline: "*Russia's anthem sounded in the streets of Italy*"[23].

The Russian media did not explain that the music in the video appears from inside the office of an organisation that the BBC article describes as "*neo-fascist*" and that the person behind the video is an activist with ties to Russia.

In its article, the BBC showed that two different videos with the Russian anthem, which circulated in the Russian media, are, in fact, recordings of the same event, but from different angles.

At the same time, with the help provided, Italy was also the target of cyber-attacks, as well as the whole of Europe.

Russian cyber operations

Cyber operations are one of the most important areas in the information warfare that the Russian Federation is waging against the background of the SARS-CoV-2 virus pandemic.

Cybercriminals are taking advantage of the growing time people spend online because of the new measures taken by member states to stop the spread of the virus.

European Commission President Ursula von der Leyen warned on 24 March about a significant increase in cybercrime in the EU in the context of the Covid-19 pandemic[24].

Cybercriminals are taking advantage of the growing time people spend online because of the new measures taken by member states to stop the spread of the virus.

The first group of hackers sponsored by the Kremlin to be employed on this front was the Hades group[25], which is rumoured to operate outside the Russian Federation, and with a link to the APT28 group, one of the most famous cyber espionage groups in the Russian Federation. According to Chinese cybersecurity company QiAnXin, Hades hackers launched a campaign in mid-February, when they hid a Trojan virus in documents containing the latest news about Covid-19. The documents were sent to targets in Ukraine, disguised in e-mails from the Public Health Centre of the Ministry of Health of Ukraine[26].

[23] *На улицах итальянских городов прозвучал гимн России*, 26.03.2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii retrieved on 15 April 2020.

[24] *EU Commission Warns of Increased Cybercrime during Coronavirus Crisis*, VOA News, 24.03.2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus retrieved on 15 April 2020.

[25] Cătălin Cîmpănu, *State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect their Targets*, 13.03.2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/ retrieved on 16 April 2020.

[26] *Ibid*.

An Europol report[27] in March also confirms what has already been listed, highlighting the fact that cybercrime has increased significantly during this period. Europol has been monitoring the impact of the *Covid-19* pandemic on the cybercrime landscape from the outset and has published an updated threat assessment on potential further developments in this area of crime.

The main findings of this eval u ation are: the impact of the SARS-CoV-2 virus pandemic on cybercrime was most visible compared to other criminal activities; criminals active in the field of cybercrime have been able to adapt quickly and capitalize on the anxieties and fears of their victims; *phishing* a nd *ransomware* campaigns are launched to exploit the current cris is and are expected to continue to grow in scope and scale; both criminal organisations, states, and state-backed actors seek to exploit the public health crisis to promote geopolitical interests[28].

It can be seen that during the SARS-CoV-2 virus pandemic, taking as a theoretical basis the NATO definition of information operations, the Russian Federation used mainly *information activities to create the desired effects on the will, understanding and capabilities of different audiences*. We also observe the planning and execution of influencing activities, activities against command and control capabilities, and information protection activities.

During the SARS-CoV-2 virus pandemic, taking as a theoretical basis the NATO definition of information operations, the Russian Federation used mainly information activities to create the desired effects on the will, understanding and capabilities of different audiences. We also observe the planning and execution of influencing activities, activities against command and control capabilities, and information protection activities.

CONCLUSIONS

Although the threat posed by the scale of this pandemic is real and not negligible, the Russian Federation sees this catastrophe as an opportunity to promote and develop plans to carry out information warfare/operations against the West amid the Covid-19 pandemic.

The spread of the SARS-CoV-2 virus has provided a new battlefield in which information warfare/operations is/are the most advanced weapon, currently benefiting from a much faster speed of spread, as well as a wide range of action, contributing decisively to rapidly model and influence both the opinions and actions of target audiences.

[27] *Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic*, 03.04.2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic retrieved on 16 April 2020.

[28] *Ibid.*

A stake for the Russian Federation in this context is the relationship with Italy, which comes at a time when this country is vulnerable. The growing interest of the Russian Federation in the EU and the provision of assistance to Italy are concrete elements for the implementation of information warfare/operations against the EU and member countries.

From the comparative analysis of the implementation of the domains of information warfare/operations during the Cold War with the specific period of the SARS-CoV-2 virus pandemic, we can see the transition from partial use of information activities specific to the Cold War to the use of all information activities, *to create the desired effects on the will, understanding and capabilities of different audiences*. The typology of the messages used is not a new one, but what is different now is the execution of increasingly intrusive information warfare/operations and use thereof not only to destabilize the US, but also the European Union.

We also consider that the actions subject to the information warfare/operations, carried out by the Russian Federation, are likely *to intensify and develop*, seeking to identify new vulnerabilities, given the countermeasures already taken by the European Union authorities and the US.

As the Russian Federation invests heavily in artificial intelligence research programs, security experts are already describing the new concept of fake news, which will be initiated by the technological capacity of artificial intelligence to faithfully reproduce the voice of the individual, as a human being, as a new field of information warfare/operations of the future.

The spread of the SARS-CoV-2 virus has provided a new battlefield in which information warfare/operations is/are the most advanced weapon, currently benefiting from a much faster speed of spread, as well as a wide range of action, contributing decisively to rapidly model and influence both the opinions and actions of target audiences.

BIBLIOGRAPHY

1. ***, AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
2. ***, S.M.G.-66, *Doctrina operațiilor informaționale*, București, 2017.
3. Cătălin Cîmpanu, *State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect their Targets*, 13 March 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/
4. Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 5 April 2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship

5. Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 April 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/
6. Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016.
7. Jacopo Iacoboni, *La Stampa*, 25 March 2020, *Coronavirus, la telefonata Conte-Putin agita il governo: "Più che aiuti arrivano militari russi in Italia",* https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327
8. Filippa Lentzos, *The Russian disinformation attack that poses a biological danger*, 19 November 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/
9. Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, vol. 57:205-227, https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618
10. Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 March 2011, http://www.rferl.org/articleprintview/2345202.html
11. Vicky Peláez, *Scientists: coronavirus would be a weapon of biological warfare*, 13 February 2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/
12. Douglas Selvage, Christopher Nehring, *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*, 22 July 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids
13. Faruk Zorlu, *Covid-19: Infodemic spreads faster than pandemic*, 31 March 2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381
14. *A New Chinese Coronavirus Was Likely Elaborated in NATO biolabs,* https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/
15. *Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic*, 3 April 2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
16. *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/
17. *EU Commission Warns of Increased Cybercrime During Coronavirus Crisis,* VOA News, 24 March 2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus
18. *На улицах итальянских городов прозвучал гимн России*, 26 March 2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii
19. *NATO Uses COVID-19 to Mobilise Western Military Forces against Russia*, 19 March 2020, interview with Alexander Artamonov conducted by Novorossia news agency, https://novorosinform.org/808651
20. *The US Defender 2020 Military Manoeuvre Is Explicitly Directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia after Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen,* https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title.

BIOLOGICAL WEAPONS AND PANDEMIC VECTORS

*Alba I.C. POPESCU, PhD**

"Carol I" National Defence University, Bucharest

Biological warfare is not an invention of the modern age. It has been practised since ancient times, when the Hittites sent plague-sick people to Egyptian camps to decimate their enemies before the battle. The difference between the epochs is made only by current technology, capable of multiplying, selecting, diversifying and hybridising the vectors of biological warfare. Thus, at present, a bacterium, grown in a laboratory-transformed pantry, can be more lethal than any chemical weapon.

Considering that, in the modern age of public access to information, the line between spontaneous, natural pandemic and biological attack followed by the outbreak of a pandemic is narrowing, the vectors of a natural pandemic can always become, in the eyes of the public, vectors of a biological attack. Conversely, until the discovery of the "zero patient" – in which natural genomic mutations occurred – any biological weapon can be considered a "natural mutation" responsible for triggering a pandemic with devastating effects. Therefore, what are the characteristics of a biological weapon? What are the main categories of biological weapons? What are the main pandemic vectors?

Keywords: pandemics, biological warfare, pandemic vectors, phytoagents, Covid-19.

* The author graduated from *"Carol Davila"* University of Medicine and Pharmacy in Bucharest, being the recipient of a master degree in public health. For many years, she worked in Africa, where she dedicated to combating AIDS, tuberculosis and malaria epidemics.

Motto: "Influenza viruses have always spread very fast ..., this is a disaster that is about to happen".
Peter C. Doherty, immunologist, laureate of Nobel Prize in Medicine

INTRODUCTION

Biological warfare is not an invention of the modern age. It has been practised since ancient times, when the Hittites sent plague-sick people to Egyptian camps to decimate their enemies before the battle. The difference between the epochs is made only by current technology, capable of multiplying, selecting, diversifying and hybridising the vectors of biological warfare. Thus, at present, a bacterium, grown in a laboratory-transformed pantry, can be more lethal than any chemical weapon. That is why the biological weapon is also called *"the nuclear bomb of the poor"*[1]. Considering that, in the modern age of public access to information, the line between spontaneous, natural pandemic and biological attack followed by the outbreak of a pandemic is narrowing, the vectors of a natural pandemic can always become, in the eyes of the public, vectors of a biological attack. Conversely, until the discovery of the *"zero patient"* – in which natural genomic mutations occurred – any biological weapon can be considered a *"natural mutation"* responsible for triggering a pandemic with devastating effects. Therefore, *what are the characteristics of a biological weapon? What are the main categories of biological weapons? What are the main pandemic vectors?*

In the modern age of public access to information, the line between spontaneous, natural pandemic and biological attack followed by the outbreak of a pandemic is narrowing, the vectors of a natural pandemic can always become, in the eyes of the public, vectors of a biological attack.

WHAT ARE MICROORGANISMS?

According to the *Encyclopaedic Dictionary*, microorganisms are *"animal or plant organisms of microscopic size (...) widespread in air, water, soil, having an important role in the circulation of substances*

[1] *The Myth of Biological Weapons as the Poor Man's Atomic Bomb*, in *Bulletin of the Atomic Scientist*, 18 March 2015, https://thebulletin.org/roundtable_entry/the-myth-of-biological-weapons-as-the-poor-mans-atomic-bomb/, retrieved on 21.04.2020.

in nature"[2], which, depending on their effects on humans, animals and plants, may be:

- saprophytes – beneficial, make up the soil microflora and microfauna and intervene in the homeostasis of the environment in which they develop, some being used in the food, pharmaceutical industry (dough preparation, wine, vinegar etc. making, preparation of yogurts, antibiotics and vitamins etc.) and in genetic engineering;
- pathogenic – cause diseases in plants, animals and humans.

Microorganisms form a very large and heterogenous group of microscopic organisms, with different morphology and biological activity, structured as follows[3]:

- *Bacteria* – prokaryotic microorganisms in the class of *Bacteria*, with a length of several micrometres, with various morphology (spherical, elongated, spiral, polymorphic). Because they do not have a nuclear membrane and nucleoli, having a nucleoid instead of a nucleus, which limits their ability to survive independently, they live in symbiotic or parasitic relationships with humans, plants and animals. They can be real eubacteria/bacteria, with a fine cell wall, gram-negative or with a thick cell wall, gram-positive and mycoplasmas, without a cell wall (mycoplasmas);
- *Archaea* – single-celled, anucleate microorganisms belonging to the class of *Archaea.* They are found in many habitats, in the soil, oceans (plankton arch), in the human colon or human navel. No pathogenic archaea is known;
- *Microscopic fungi* (moulds and yeasts) – are eukaryotic microorganisms belonging to the class of *Fungi*, one of the three major classes of *Eukaryote*. They have complete nucleus and they can be saprophytes, parasites or symbiotics with plants (mycorrhiza) or with blue-green algae (lichens);

[2] Marcel D. Popa *et al.*, *Dicționar Enciclopedic*, Editura Enciclopedică, 1993-2009, https://dexonline.ro/definitie/microorganism, retrieved on 10.04.2020.

[3] Valeria Firă, Maria Năstăsescu, *Zoologia nevertebratelor*, Editura Didactică și Pedagogică, București, 1977.

- *Microalgae or microphytes* – single-celled eukaryotic microorganisms present in freshwater and marine systems, including sediments. They can exist individually, in chains or in groups, and can reach sizes from a few micrometres to a few hundred micrometres. Capable of photosynthesis, they produce about half of atmospheric oxygen. No pathogenic microalgae is known;
- *Protozoa* – the simplest single-celled eukaryotic organisms in the subclass *Protozoa*, make the connection between plants and animals. They live in the aquatic/liquid environment, some can reach visible dimensions, of the order of centimetres. 40 species of protozoa are pathogenic to humans;
- *Viruses* – are acellular entities, exclusively parasitic and pathogenic, on the border between living and non-living. They are made of genetic material (DNA or RNA), invisible to the light microscope, without the ability to self-reproduce outside a parasitic cell;
- *Infectious agents* (viroids, prions) – not considered microorganisms, they are infectious agents of a protein nature, free of any type of nucleic acid.

Bacteria, fungi, protozoa, viruses and subviral infectious agents are pathogenic to humans, plants and animals, the diseases caused by pathogenic microorganisms being called infectious diseases.

As we can deduce from the above classification, only bacteria, fungi, protozoa, viruses and subviral infectious agents are pathogenic to humans, plants and animals, the diseases caused by pathogenic microorganisms being called *infectious diseases*.

The pathogenic microbial agent has a number of properties, such as[4]:

- **Pathogenicity**: the ability of a microorganism to produce an infectious disease in a receptive host. The infection generated by the pathogenic microorganisms in animals is called *zoonosis*, when affecting animals, and *anthropozoonosis*, when affecting humans.

[4] *General Notions on Pathogenicity and Virulence*, https://www.scribd.com/doc/270695407/Notiuni-Generale-de-Patogenitate-Si-Virulenta, retrieved on 10.04.2020.

- **Virulence**: the minimum amount of microorganism or its product capable of causing the disease or death of the biological testing system.

It represents a quantitative indicator of pathogenicity, dependent on three characteristics of the microbial agent, namely:

1. ***Infectiousness*** – the ability of the pathogenic microorganism to penetrate, localise and multiply in the host organism, despite the attacks of the immune system, and to produce a primary outbreak of infection;
2. ***Invasiveness*** or *aggressiveness*, namely the ability of the pathogenic microorganism to overcome, through own means, the epithelial barriers, and to penetrate and multiply in the host tissues;
3. ***Toxicity*** – the ability of the microbial agent to produce toxins. It is an essential property of the bacterial pathogenic mechanism.

There are three levels of virulence:

- *increased virulence*, specific to microbial strains that produce infections with severe clinical course;
- *diminished virulence*, specific to microbial strains that produce mild forms of disease;
- *attenuated virulence*, specific to the strains used to prepare vaccines.

Of the multitude of pathogenic microorganisms, very few are susceptible to generate pandemics, due to the properties of virulence and pathogenicity and, especially, due to the development of defence mechanisms in host organisms. Usually, pandemics[5] are produced by microorganisms capable of generating new strains, having increased pathogenicity and virulence. In general, the most susceptible to naturally develop such strains capable of generating pandemics are *RNA*-type viruses, in which the frequency of genetic mutations increases with each multiplication in the nucleus of the host cell.

[5] Epidemics present on minimum five continents.

However, there is also the possibility of human intervention, in the laboratory, on microbial genomes, in order to amplify these features and to transform microorganisms in biological weapons.

There are also other criteria for classifying pathogens, depending on:

- the target kingdom: phytoagents (acting on the plant kingdom – plants, shrubs and trees) and zoo/anthropoagents (acting on the animal kingdom – humans, animals, birds, insects);
- the effects on the host organism: haemolytic, cytolytic, necrotic etc. agents;
- the route of transmission: digestive, aerial, haematological etc.

BIOLOGICAL WEAPONS

What Are the Characteristics of a Biological Weapon?

According to the definition agreed by the World Health Organisation *"biological weapons are microorganisms like viruses, bacteria, fungi, or other toxins that are produced (in laboratory) and released deliberately to cause disease and death in humans, animals or plants"*[6]. They represent difficult challenges for healthcare services, economy, society, because of the large number of deaths/destructions in the livestock and harvest, they can generate in a short period of time.

According to the definition agreed by the World Health Organisation "biological weapons are microorganisms like viruses, bacteria, fungi, or other toxins that are produced (in laboratory) and released deliberately to cause disease and death in humans, animals or plants".

Biological weapons represent a category of a larger class of weapons, called *Mass Destruction Weapons*, which also includes chemical, nuclear and radiological weapons.

The microorganisms transformed into biological weapons are **multiplied by biotechnology,** and **the genetic manipulation** induces **characteristics they do not initially possess,** namely:

- high pathogenicity;
- high infectivity;
- high virulence;
- multiple resistance to antibiotics, antivirals or antifungals;
- period of highly contagious asymptomatic incubation;

[6] *Biological Weapons,* World Health Organisation, https://www.who.int/health-topics/biological-weapons#tab=tab_1, retrieved on 10.04.2020.

- action on numerous systems and apparatuses in the human body;
- increased lifespan of the microorganism outside the reservoir organism;
- duration of action limited in time (to allow for the subsequent invasion of the respective depopulated territory);
- selective tropism of the biological agent to some population groups etc.

What must be kept in mind is that, in the case of a biological weapon, one can never identify the *"zero patient"* in whose body the lethal mutation occurred. *The identification of the "zero case" is the indisputable proof that a pandemic disaster broke out naturally*. However, although it is possible, it is not necessary for the *"zero patient"* to be identified in the event of a natural pandemic, a situation which may give rise to suspicions related to its origin. As a consequence, there is a very narrow boundary between natural pandemics and those produced by biological attacks, a limit shattered only by the identification of the *"zero case"*.

Unlike other weapons of mass destruction, a biological weapon can be manufactured in small spaces, being easy to transport, impossible to detect, as it is colourless, tasteless, and invisible.

The impact produced by these microorganisms on the human/animal population depends on several factors, as follows:

- the incubation period, in which the body becomes an asymptomatic and contagious reservoir, should be as long as possible;
- the route of transmission, which can be digestive, aerial or haematological;
- the existence or not of antidotes or effective treatments;
- the costs and duration of treatments;
- the death rate in the first 24-72 hours following the outbreak of the disease.

The most dangerous routes of transmission, because of the great number of individuals that can be infected, are the digestive and the aerial ones.

Unlike other weapons of mass destruction, a biological weapon can be manufactured in small spaces, being easy to transport, impossible to detect, as it is colourless, tasteless, and invisible.

In equal quantities, biological weapons are far more deadly than chemical ones. For instance, the lethal dose of botulinum toxin is 0.1 micrograms when ingested and 5 micrograms when inhaled. The lethal dose of *VX Lethal Nerve Agent*, the most toxic neuromuscular blocking agent, is 1,000 micrograms when inhaled, being 200 times higher than that of botulinum toxin[7]. Moreover, the proliferation of such types of weapons occurs naturally, as they are living organisms.

Therefore, a high-performance biological weapon can easily trigger a global pandemic, having demographic, social and political effects that are difficult to manage, surpassing, because of the complexity of consequences, any other weapon of mass destruction.

Although the processing, production and storage of biological weapons are prohibited by the *Convention of 10 April 1972*[8], the reality has shown the continuation of the research and production in the field, even in improvised laboratories, as it was the case of the Japanese cult *Aum Shinrikyo*, led by Shoko Asahara, which had begun the production of anthracic bacillus[9], for terrorist purposes. In this regard, biological terrorism or *"**bioterrorism** represents the threat or use of biological weapons – microorganisms or biological toxins, capable of causing disease or death of humans, animals, insects and plants – in order to meet political/economic objectives"*[10].

What Are the Main Categories of Biological Weapons?

1. Biological weapons acting on human health

The Centre for Disease Control and Prevention Atlanta (C.D.C. Atlanta)[11] classified biological weapons acting on humans in three categories, depending on pathogenicity, morbidity, mortality

[7] Eric Croddy, James J. Wirtz, *Weapons of Mass Destruction: Chemical and Biological Weapons*, ABC CLIO, 2005, p. 54.

[8] *Convention of 10 April 1972 on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction*, http://legislatie.just.ro/Public/DetaliiDocument/28190, retrieved on 29.05.2020.

[9] *Aum Shinrikyo: The Japanese Cult behind the Tokyo Sarin Attack*, BBC News, 06.07.2018, https://www.bbc.com/news/world-asia-35975069, retrieved on 29.05.2020.

[10] Alba Iulia Catrinel Popescu, *Jucătorul din umbră*, Editura Militară, București, 2016, p. 229.

[11] Centers for Disease Control and Prevention (C.D.C.) Classification of Bioterrorism Microorganisms, Part 3 of 5, Johns Hopkins Bloomberg School of Public Health, 2006, http://ocw.jhsph.edu/courses/BiologicalAgentsOfWaterAndFoodborneBioterrorism/PDFs/WaterFoodTerror3.pdf, retrieved on 29.10.2015.

and easiness to procure, produce and disseminate in the environment as follows:

- *class A* (easily disseminated and transmitted from person to person, highly pathogenic, very high mortality, can generate public panic and civic insubordination, having major impact on public healthcare services, economy, social relations, political stability):
  - aerial transmission: *Bacillus anthracis* (anthrax), *Variola major* (smallpox), *Yersinia pestis* (plague), *Francisella tularensis* (tularaemia), *filoviridae* (Ebola and Marburg haemorrhagic fevers), *arenaviridae* (Lassa and Argentinian haemorrhagic fevers);
  - digestive transmission: neurotoxin *Clostridium botulinum* (botulism);
- *class B* (relatively easy to disseminate, moderate morbidity, low mortality, can generate public panic, having major impact on healthcare services and economy, as well as on the other sectors of the society):
  - aerial transmission: *Brucella sp.* (brucellosis), *Coxiella burnetti* (Q fever), *Rickettsia prowazekii* (exanthematous typhus), *alphaviridae* (viral encephalitis), *Burkholderia mallei* (snot), *Ricinus communis toxin* (haemorrhagic diarrhoea), *Clostridium perfringens* epsilon toxin (toxic infections, gaseous gangrene), *Staphylococcus aureus* B enterotoxin (sepsis);
  - digestive transmission: *Salmonella sp.* (salmonellosis), *Vibrio cholerae* (cholera), *Shigella dysenteriae* (dysentery), *Cryptosporidium* (cryptosporidiasis), *Escherichia coli O157: H7* (entero-haemorrhagic infection), *Noroviridae* (viral gastroenteritis);
- *class C* (easy to procure, produce and disseminate, high morbidity and mortality, having major impact on the population): *Koch bacillus* resistant to anti-tuberculosis therapy (tuberculosis), *Nipah viridae* (viral encephalitis), *hantaviridae* (cardiopulmonary syndrome), *Flaviviridae* (yellow fever),

viruses of haemorrhagic fevers and encephalitis, transmitted by tick bite.

The discharge of certain bacteria, such as those that cause dysentery, typhoid fever and especially botulism, in the drinking water supply system of a metropolis, or the aerial dissemination by airplanes, drones or aerosol devices, of microorganisms such as those that cause influenza, smallpox or anthrax can generate uncontrollable epidemics.

Such an epidemic episode, we were already confronted with, when it was about to be transformed into a source of biological weapons for terrorist networks, occurred in 2014, in the west of Africa. Then, in Guinea, Liberia and Sierra Leone, it was an outbreak of *Ebola* haemorrhagic fever epidemics (included by *C.D.C. Atlanta* among class A biological agents). The main concerns were related to the possibility for Jihadist structures to procure viral strains from the secretions belonging to ill people or to transform infected militants in biological vectors, subsequently sent, using the illegal migration networks, in public transportation means, railway stations and international airports or in large Western urban agglomerations[12]. Concerns were heightened by the state of panic and civic insubordination of the disaster-stricken population, as well as of the inability of African governments to manage the situation effectively. Under those circumstances, amid the major risk of multiplication and spread of disease to other West African states, the United States of America decided to send to Liberia more than 2,500 troops from the *101st Airborne Division* as part of *United Assistance* operation to provide aid to the local governments involved in counteracting the epidemic. The US military's mission was to contain outbreaks and counteract local panic, as well as to support the work of medical and paramedical personnel within the *United States Agency for International Development (U.S.A.I.D.)*. During the five-month mission, between 25 October 2014 and 27 February 2015, treatment centres were built, mobile laboratories were established,

ROMANIAN MILITARY THINKING

The discharge of certain bacteria, such as those that cause dysentery, typhoid fever and especially botulism, in the drinking water supply system of a metropolis, or the aerial dissemination by airplanes, drones or aerosol devices, of microorganisms such as those that cause influenza, smallpox or anthrax can generate uncontrollable epidemics.

[12] Bruce Dorminey, *Ebola as ISIS Bio-Weapon?,* Forbes, 05.10.2014, http://www.forbes.com/sites/brucedorminey/ 2014/10/05/ebola-as-isis-bio-weapon/, retrieved on 26.09.2015.

and more than 1,500 local health workers participated in specialisation courses held by US military personnel[13,14].

Yet the biological weapon is not just for humans. It can also attack the rest of the ecosystem, from plants to animals, birds, fish and insects, in this case, the purpose being mainly an economic one, to destroy food sources.

The biological weapon is not just for humans. It can also attack the rest of the ecosystem, from plants to animals, birds, fish and insects, in this case, the purpose being mainly an economic one, to destroy food sources.

2. Phytoagents

The destruction of crops and food reserves was an ancient military tactic, also used in modern times, the Vietnam War (1955-1975) being an example in this regard. The effects of a massive infestation are measured in thousands of hectares of destroyed crops, famine, destruction of the ecosystem by the disappearance of trophic links, destruction of livestock, internal instability, high economic, human and animal costs, especially when such a plague occurs against the background of prolonged droughts or in overpopulated regions, the vulnerability of the country to an unforeseen event or conflict.

Phytoagents can be microorganisms or insects: locusts, Colorado potato beetles, wild bees, Japanese wasps, butterfly species etc.

A classic example of microbial phytoagent is the fungus *Prycularia oryzae cavara*, also called *rice agent*, responsible for the disease named *"rice fever"*[15]. Appearing in a field, within few hours, through the spores, it can infest the entire area, resulting in the death of all the plants. For instance, such an attack, of an *agroterrorist* type, focused on the rice crops in Asia or Australia, can result in the death of millions of people because of starving, the explosion of the food prices, and huge global financial imbalances.

[13] Anthony P. Cardile, Clinton K. Murray, Christopher T. Littell, Neel J. Shah, Matthew N. Fandre, Dennis C. Drinkwater, Brian P. Markelz, Todd J. Vento, *Monitoring Exposure to Ebola and Health of U.S. Military Personnel Deployed in Support of Ebola Control Efforts – Liberia*, 25 October 2014-27 February 2015, *Morbidity and Mortality Weekly Report (MMWR)*, Centers for Disease Control and Prevention, 03.07.2015, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6425a2.htm, retrieved on 29.10.2010.

[14] Alba Iulia Catrinel Popescu, *op. cit.*, pp. 229-231.

[15] *Rice-Detailed Study of Diseases*, http://www.ikisan.com/links/ap_riceDetailedStudyofDiseases.shtml, retrieved on 01.01.2016.

Currently, there are more than 200 such phytoagents specialised in one type of plant: cereal, vegetable, fruit, shrub, tree etc.

3. Zooagents

Zooagents have as target organisms both humans and other mammals, birds, insects or fish. They are extremely numerous and diverse. Annually, new species highly resistant to antibiotics, antivirals and antifungals emerge, and their effects on public health and economy are devastating, as they can generate pandemics having huge demographic consequences and direct implications on the vast majority of the national power components, resulting in the vulnerability of the affected states and the area instability. When infesting livestock, fish stocks or birds, the consequences are epizootics which, especially in regions unsuitable for agricultural crops, lead to famine, with all the related social manifestations.

Zooagents have as target organisms both humans and other mammals, birds, insects or fish.

Rinderpest or **cattle plague** is an epizootic caused by the highly pathogenic *Rinder virus*, which affects both cattle and other ruminant herbivores. As in the case of swine fever/plague, the disease can be transmitted very easily, and can affect an entire herd in a few days.

The economic consequences of a widespread epizootic, even without the characteristics of a biological weapon, are in the order of tens of millions of dollars. For example, **African swine fever** or Montgomery's disease, a highly contagious and severe febrile haemorrhagic viral disease, has caused enormous damage, suffice it to mention:

- the episode in the USA, from 1975, resulting in losses of approximately $ 65 million;
- the outbreaks in Romania in 2007, which cost Smithfield Company about $ 12 million;
- the epizootic from 2018-2019, which led to the destruction of some pig breeding plants and the stopping of some national programmes for the revitalisation of the Romanian Bazna and Mangaliţa pig breeding.

This is how an epizootic can cause the economic collapse of a region and the cessation of national programmes, especially when it becomes recurrent.

Other classic examples of epizootics are **mad cow disease** or **bovine spongiform encephalopathy**, which has resulted in loss of life and huge economic losses by mass slaughter of livestock in areas adjacent to a proven case, and the well-known **avian influenza**, which has caused economic losses, including in our country, by mass slaughtering the bird population in large regions of the country.

Avian influenza is the first pandemic/epizootic that has shown that the alarm signals sounded by the World Health Organisation (WHO) are not just meaningless discussions. The mode of transmission of the disease, through migratory birds, which can travel thousands of miles during a journey, is reminiscent of the air transportation system, through which a patient, an active reservoir of microbes, can reach, in a few hours, another continent, it can transmit the disease.

Avian influenza is the first pandemic/ epizootic that has shown that the alarm signals sounded by the World Health Organisation are not just meaningless discussions.

The fact that the United Nations (UN) appointed Dr David Nabarro[16] as *UN Coordinator of Avian and Human Influenza* [17] on 29 September 2005 demonstrated the concern about the risk of a pandemic, the consequences of which would involve, in addition to the potential loss of human lives, economic and ecological consequences, by involving food chains and ecosystems across bird migration routes.

According to former director general of the World Health Organisation, Margaret Chan, *"no country is prepared for the possibility of an avian flu pandemic. There will not be enough reserves, neither of medicines, nor of sanitary material such as masks (...), and the attack rate could reach 20% of the population"*[18]. The statement, dated November 2007, is still valid today, when the Covid-19 coronavirus wreaks havoc.

[16] *WHO Expert to Work with the UN System on Avian and Human Influenza,* World Health Organisation, https://www.who.int/mediacentre/news/releases/2005/pr45/en/, retrieved on 01.04.2020.

[17] System that reunites international organisations such as FAO/OIE – monitoring animal health, WHO – epidemiology and human health, UNEP – monitoring world migratory birds, UNICEF – public information campaigns, OCHA/WFP/UNHCR – planning, warning and humanitarian aid, UNDP – ensuring multi-sector government planning.

[18] See https://www.who.int/mediacentre/influenzaAH1N1_presstranscript_20090611.pdf, retrieved on 05.04.2020; Alexandra Sandru, *Pericolul aviar: Crezi că ne vom confrunta cu o pandemie? (sondaj),* ziare.com, 29.11.2007, http://www.ziare.com/social/capitala/pericolul-aviar-crezi-ca-ne-vom-confrunta-cu-o-pandemie-sondaj-185674, retrieved on 05.04.2020.

PANDEMIC VECTORS

What Are the Most Common Pandemic Vectors?

a) Viruses

The human flu. The pandemic episode at the beginning of the last century, known as the S*panish flu*, resulted in 400 million diseases and 50 million deaths, the most affected being the 20-40 age bracket. The explanation is related to the fact that this age bracket is the one involved in social activities, knowing that the flu virus is transmitted through coughing, sneezing or contact with body fluids up to a distance of 10 meters from the recipient. Practically, in one year, 1918, the number of victims of this pandemic was higher than the loss of life in the world conflagration that had just ended, and the economic costs induced by the pandemic, combined with the post-conflict destruction, contributed to the recession in 1920s. Subsequently, in 1957 and 1968, there were two more pandemic episodes, known as the *Russian flu* and the *Hong Kong flu*. In the face of this reality, the WHO developed the annual preventive vaccination programme against influenza. It should be noted that the influenza virus undergoes mutations from one year to another, therefore the annual immunisation, corresponding to the new viral genotype, is mandatory.

These mutant viruses are extremely dangerous, because they take pathogenic elements from the original viruses, neither humans nor animals have immunity to them, and there are no vaccines prepared for such a situation.

WHO officials have repeatedly pointed out that it is likely that a new influenza pandemic will be triggered by a hybrid avian-human virus, easily transmitted to humans, caused by a nuclear combination in a human organism that has suffered double infection[19]. These mutant viruses are extremely dangerous, because they take pathogenic elements from the original viruses, neither humans nor animals have immunity to them, and there are no vaccines prepared for such a situation. In this regard, WHO representatives stated that, *"if the virus undergoes mutations that will provide it with the ability to spread*

[19] *OMS atrage atenția asupra riscului unei pandemii de gripă*, Rompres, 17.10.2007, http://www.romedic.ro/stiri-medicale/Stiri_generale_0341/OMS_atrage_atentia_asupra_riscului_unei_pandemii_de_gripa_04178.html, retrieved on 08.01.2009; Neeti Mittal, Bikash Medhi, *The Bird Flu: A New Emerging Pandemic Threat and Its Pharmacological Intervention*, in *International Journal of Health Sciences*, 2007, July https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3068632/, retrieved on 10.04.2020.

from one person to another, it is difficult to find a historical comparison with what will follow". The current pandemic, with the Covid-19 coronavirus, begins to fulfil the *"prophecy"* of WHO specialists.

Severe Acute Respiratory Syndrome-SARS is relatively recently known by the doctors at the forefront of the fight against major epidemics, more or less naturally occurring. In 2002, in the southern Chinese province of Guandong, a series of rapidly evolving respiratory infections were identified, through pneumonia resistant to any treatment. The reservoir species of this mutant virus has not been known yet. The fact that this epidemic has not reached global proportions is due to doctors from international organisations such as the WHO or *Médecins Sans Frontières* (Doctors Without Borders), who managed to stop this scourge in 2003. About 800 people have died as a result of the SARS epidemic, including doctors who worked to stop the disaster[20].

Enterovirus 71 infection. In May 2008, an epidemic broke out in China, mostly affecting children under the age of six. The infection was called *"hand-foot-mouth"* disease due to herpes rashes in the mouth and eczema on the hands and feet. Accompanied by high fever and diarrhoea, this enterovirus is extremely severe due to pathogenicity and infectivity. So far, researchers have not been able to discover the pathogenic mechanism of this virus[21].

HIV-AIDS infection. Huge volumes have been written about this infection, huge sums have been allocated for the discovery of the virus involved in the onset of this disease, for finding a treatment, for information campaigns, for the safety industry, movies have been made, monuments have been erected, in a word, this infection was the emblem of the last century, a disease that has caused great anxiety in mankind and brought the greatest profits to the medical and sanitary supplies industries. The most affected continent was Africa,

[20] *Feature: Colleagues and Patients Honor Doctor Killed by SARS (2),* http://www.highbeam.com/doc/1P2-13415220.html, retrieved on 02.04.2020.

[21] C. Chi, Q. Sun, S. Wang, Z. Zhang, X. Li, C.J. Cardona, Y. Jin, Z. Xing, *Robust Antiviral Responses to Enterovirus 71 Infection in Human Intestinal Epithelial Cells*, 16 May 2013, US National Library of Medicine National Institutes of Health, https://www.ncbi.nlm.nih.gov/pubmed/23685430, retrieved on 10.03.2020.

the place of many horrors and a space for confrontation of the great global economic interests in the field of oil, strategic ores, diamonds, uranium etc. Although the most powerful charitable organisations are financially involved in combating this scourge and large multinational companies are successfully marketing their latest technical wonders in identifying and assessing the frightening virus infection, the results on the ground are still negative.

During one of the many conferences held annually on acquired human immunodeficiency retrovirus infection, *Médecins Sans Frontières* released a number of realities on the ground, saying: *"A nurse in Malawi keeps 400 patients alive by giving them treatment, but she is only paid three dollars a day"* – a statement by Dr Moses Massaquoi, coordinator of the humanitarian organisation in Malawi[22] – and that *"it is devastating to sit and see how people get worse and worse – and how they die sometimes – while waiting for weeks and even months before being treated simply because there are not enough health workers"* and those who exist are *"overworked, underpaid and undervalued"* – said Dr Mit Philips on the situation of doctors and average staff in states with a high prevalence of the disease, quoted by AFP. Indeed, the scourge of the century is far from being limited or controlled. Every day, new cases occur, the disease has exceeded the continental dimensions, becoming the most *"successful"* pandemic that has affected the Western as well as the Asian or African world. The fact that this disease has affected both the rich, the beautiful and the famous, as well as the poor, has shown, once again, that in the face of disease and death, we are all equal and that a microorganism, the fruit of unknown circumstances, ends up taking its toll, regardless of the name of its victim.

In the WHO annual report in 2007[23], it was mentioned that the risk of a global epidemic was higher and higher. In the report it was stated

ROMANIAN MILITARY THINKING

The most affected continent was Africa, the place of many horrors and a space for confrontation of the great global economic interests in the field of oil, strategic ores, diamonds, uranium etc.

[22] *Mind the Deadly Gaps: Health Care Worker Shortages in Southern Africa Causing Fatal Delays in Bringing AIDS Care to Those in Urgent Need*, https://www.internationalbudget.org/wp-content/uploads/2011/04/newsletter46.pdf, retrieved on 02.04.2020.

[23] *The World Health Report 2007 – A Safer Future: Global Public Health Security in the 21st Century,* WHO, https://www.who.int/whr/2007/en/, retrieved on 02.04.2020.

that *"in our world that is highly interconnected, new diseases occur with an unprecedented frequency, often with the possibility to cross the border and spread rapidly"*, the officials mentioning the emergence of **39 infectious diseases since 1967 up to the present moment**, among them HIV-AIDS, SARS, Ebola, enterovirus 71 etc. and of more than 1,100 epidemic episodes in different regions of the world. It was also mentioned that *"considering that approximately 2.1 billion people travel by airlines annually, the risk of a global epidemic is very high"*. Moreover, the WHO officials required for the world's states to secure sufficient stocks of vaccines and emergency medicines. Unfortunately, their appeal had gone unheeded. In 2020, humanity is as exposed to the risks described by the WHO officials as it was before 2007.

WHO report: 39 infectious diseases since 1967 up to the present moment, among them HIV-AIDS, SARS, Ebola, enterovirus 71 etc. and more than 1,100 epidemic episodes in different regions of the world.

Smallpox killed between 300 and 500 million people in the 20th century alone. In 1967, there were 15 million illnesses and two million deaths. In the same year, the WHO launched an intensive vaccination and public information campaign on the disease, so that 10 years later, smallpox was completely eradicated. Since then, no case has been reported, as smallpox is the only contagious disease whose germs, *orthopoxviridae*, have been completely eliminated from the environment. It is very contagious, being transmitted through direct contact or through contaminated objects. After a relatively long period of asymptomatic incubation, of 12-14 days, it triggers high fever, headache, violent lumbar pain and pustular rash. The vaccination and isolation of patients quickly stop the disease. As the smallpox vaccine contains attenuated germs, early vaccination is not justified, as the disease may occur if the body is weakened. Mortality varies between 20% and 50% of cases. Smallpox was the biological instrument of the genocide in 1763, when English colonists liquidated the Native American tribes in Ottawa. Smallpox-infected blankets were given as gifts to Native Americans. In two weeks, thousands of natives died[24].

In 2020, humanity is as exposed to the risks described by the WHO officials as it was before 2007.

Haemorrhagic fevers (Lassa, Ebola) are, probably, the great fear of the institutions having responsibilities in ensuring national security.

[24] Patrick J. Kiger, *Did Colonists Give Infected Blankets to Native Americans as Biological Warfare?,* History, 25.11.2019, https://www.history.com/news/colonists-native-americans-smallpox-blankets, retrieved on 03.04.2020.

The first official cases of Ebola were recorded in the region of the same name, from the current R.D. Congo, in the years 1970-1980, when numerous corpses of primates and humans were discovered, with blood dripping from dozens and dozens of wounds. The reservoir organisms have not yet been discovered with certainty, although some incriminate frugivorous bats. No effective treatment is known and no active prophylactic measures can be established. It is now known for sure that the Ebola virus is transmitted through contact with human feces and fluids from infected people. Fortunately, however, both Ebola and Lassa could not be very effective biological weapons in the hands of terrorists, as the sick die so quickly that they no longer have time to transmit the disease[25]. The characteristic of these diseases is high fever, intense muscle pain and microhaemorrhages that affect the capillaries throughout the body, which is why Ebola fever has been called *"the disease of a million cuts".* Mortality easily reaches 90% of cases in the first two weeks.

Ebola and Lassa could not be very effective biological weapons in the hands of terrorists, as the sick die so quickly that they no longer have time to transmit the disease.

Nipah virus is a recent discovery by microbiologists. In 1999, an epidemic encephalitis broke out in the Nipah region of Malaysia, killing 105 people without anyone being able to determine the cause of the disease. Virologists were able to isolate the Nipah virus, but were unable to establish the reservoir. It appears to be a zoonosis that affects humans and pigs, is transmitted through direct contact with infected fluids of humans and animals, has an incubation period of 4-18 days and, after an influenza-like prodrome, causes inflammation of the brain, followed by coma and death. There is no treatment[26]. It is included in the category of biological weapons type B.

Chimera viruses are the result of military laboratories looking for the perfect weapon. They are named after the mythical character having the same name, Chimera, the three-headed monster with a snake head, a lion head and a goat head. Like Chimera, these viruses

[25] L. Borio, T. Inglesby, C.J. Peters et al, *Hemorrhagic Fever Viruses as Biological Weapons: Medical and Public Health Management,* 8 May 2002, https://www.ncbi.nlm.nih.gov/pubmed/11988060, retrieved on 02.04.2020.

[26] *Nipah virus infection,* WHO, https://www.who.int/csr/disease/nipah/en/, retrieved on 02.04.2020.

are obtained by combining genetic material belonging to the most aggressive viruses currently available. In the 1990s, Dr Ken Alibek, a researcher in the Soviet Chimera programme, defected to the United States of America and declared before the Congress that the USSR had developed a virus that combined the pathogenicity of two of the deadliest microorganisms: Ebola and smallpox[27]. Subsequently, Alibek published some of his knowledge in the field in the book *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told from Inside by the Man Who Ran It*[28].

It is known that some armies have stocks of smallpox virus combined with the Venezuelan encephalitis virus and there is intense discussion, for the time being, at the level of conspiracy theory, about the artificial, laboratory character of HIV, as well as about the possibility of a hybrid **HIV and influenza virus, airborne transmitted**. Of course, the first question that arises in such a case is related to the consequences of the release, even accidentally, of such a weapon. What would humanity become, how could even those who finance and plan such monstrosities survive without protective equipment? We have a first answer right now, when Covid-19 wreaks havoc on the elderly population and has paralysed the world economy.

b) Bacteria

The plague, the disease that has frightened mankind for thousands of years, is caused by a bacterium, *Yersinia pestis*, and can manifest itself in two clinical forms: *bubonic plague* and *lung plague*. The route of transmission of the disease is through contact with infected body fluids and through the bites of hematophagous insects, such as fleas and lice. In the absence of treatment, in the first 24 hours after infection, mortality is 70%-90%, which makes this microbe a significant bacteriological weapon. Plague, exanthematous typhus

[27] See http://www.house.gov/jec/hearings/intell/alibek.htm, retrieved on 02.04.2009.

[28] Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told from Inside by the Man Who Ran It*, Delta; Reprint edition, 11 April 2000.

and more recently infectious panconitis with *Bartonella rochalimae*[29] are diseases transmitted by insects that parasitise rats, rodents whose number, in some urban areas of Asian countries, Africa and beyond, exceeds the number of people. The mark of the disease is an infected axillary ganglion. If the ganglion abscess drains, the patient escapes, otherwise, in the absence of adequate antibiotic treatment, he dies of sepsis.

Anthrax is a condition caused by a bacterium, *Bacillus anthracis*, which can resist in dust, in the form of spores, for up to 40 years, which is extremely important in evaluating the long-term effectiveness of such a weapon. The route of transmission is air, skin and digestive, the lung form of the disease being 100% deadly. The mark of the disease is the so-called *"black spot"*, which occurs in the skin at the site of anthrax inoculation, where an area of necrosis is created, responsible for the dark colour of the skin. Death occurs by sepsis within a few hours of inoculation, its pathogenicity being so high that, even in the case of rapid treatment, mortality is 75%.

Anthrax is a condition caused by a bacterium, Bacillus anthracis, which can resist in dust, in the form of spores, for up to 40 years, which is extremely important in evaluating the long-term effectiveness of such a weapon. The route of transmission is air, skin and digestive, the lung form of the disease being 100% deadly.

Military research on this microbe dates back to the 1980s, when both the Soviet and American armed forces accumulated stockpiles of anthrax-core missiles. In the context of the 2001 terrorist attacks, the Federal Bureau of Investigation (FBI) released information on a possible link between the 2001 anthrax attacks and people having connections with a US military centre[30].

Tularemia. The bacterium *Francisella tularensis* is one of the most infectious, being transmitted by air, digestive, blood, or by contact with contaminated animal fluids. Known as the *rabbit disease*, tularemia caused numerous casualties during the Second World War, when the German and Soviet armed forces mutually accused that they had used infected rabbits as biological weapons. The incubation

[29] *Scientists Discover 21st Century Black Plague that Spreads from Rats to Humans*, Daily Mail, 24.11.2008, https://www.dailymail.co.uk/health/article-1088887/Scientists-discover-21st-century-black-plague-spreads-rats-humans.html, retrieved on 02.04.2020.

[30] *A Study of the 2001 Anthrax Terror Attacks and the History of Biological Warfare,* 01.04.2015, https://www.fasebj.org/doi/abs/10.1096/fasebj.29.1_supplement.735.3, retrieved on 02.04.2020.

period is 3-5 days, when the infected individual becomes a reservoir, which makes the disease more dangerous. This bacterium is included in the category of biological weapons. In the 1950s, the USA, the USSR, the UK and Canada developed production units, and in the 1990s, the Swedish researchers isolated an extremely dangerous strain, resistant to antibiotics[31]. As it is sensible to solar radiation, the experts in countering bioterrorism say that a terrorist attack using Francisella could be effective only in dark and crowded areas, such as subway stations or underground walkways[32].

Botulism is a very serious paralytic disease caused by the neurotoxin of the bacterium *Clostridium botulinum*. The bacterium is common and widespread in nature, being present in a latent state, of spores, in soil and ocean sediments. If it reaches anaerobic environments, such as canned food, deep wounds or intestinal tract, spores germinate into active bacteria, which multiply and produce toxin. Clostridium botulinum produces eight types of toxins (from A to H), considered to be among the most potent toxins known at this time. For example, a highly diluted botulinum toxin A formula is used clinically as Botox and a highly diluted botulinum toxin B formula is used clinically as Myobloc[33]. Untreated, botulism causes paralysis of striated muscles, including respiratory muscles, followed by death within 24-72 hours. The fact that this bacterium is transmitted by air, skin (if there is a deep wound) and food makes it maximum dangerous. Botulinum toxins are among the most effective biological weapons, because:

Untreated, botulism causes paralysis of striated muscles, including respiratory muscles, followed by death within 24-72 hours. The fact that this bacterium is transmitted by air, skin (if there is a deep wound) and food makes it maximum dangerous.

- they are extremely powerful and lethal, being necessary infinitesimal quantities to kill a 70 kg adult (inhalation of 0.7-0.9 µg aerosolised botulinum toxin);
- some of them are relatively easy to produce and transport;
- ill people need intensive care, which cause the paralysis of the healthcare system[34].

Cholera is an extremely serious and contagious condition caused by *Vibrio Cholerae*. It is a severe acute diarrheal disease, accompanied by heavy vomiting, which causes exsiccosis – rapid dehydration of the patient through massive loss of electrolytes. Mortality exceeds 85% of cases at the outbreak of the epidemic. The pathway of vibrio transmission is digestive, feces-oral. Under natural conditions, it is an epidemic specific to poverty and underdevelopment, being transmitted either through drinking water infected with feces as a result of poor sanitation, or through the consumption of infected fish and/or water from infected running or stagnant water. At the beginning of the last century, the great Romanian scientist, Dr Ion Cantacuzino (1863 - 1934) isolated the vibrio and produced the first cholera vaccine, which was administered to Romanian troops on the front during the Second Balkan War (16 June 1913 – 18 July 1913), saving them from extinction and radically changing the fate of the war[35]. Transformed into a weapon, the cholera vibrio increases its contagiousness, virulence and pathogenicity, being included among the biological weapons of category B.

Global foodborne infections. Since 2006, the author of *The Omnivore's Dilemma: A Natural History of Four Meals*[36], American journalist Michael Pollan[37] has drawn public attention to the risk of *Salmonella* and *Coli bacillus* pandemics, following the consumption of food traded, at global level, by the large corporations in the food industry. These corporations have come to monopolise the entire manufacturing chain, from production to sale. In this regard, Pollan mentions that, in 2007, the USA was confronted with severe digestive

[31] Kristy Young Johnson, Paul Matthew Nolan, *Biological Weapons: Recognizing, Understanding, and Responding to the Threat*, Hoboken, NJ: Wiley, 2016, p. 98, https://books.google.ro/books?id=O4ebCgAAQBAJ&pg=PA98&lpg=PA98&dq=tularemia+Russia+2005+biological+weapon&source=bl&ots=d90NA_Zxoc&sig=ACfU3U3M16f5YjFVnmHFhqwaNfJv_hUHjQ&hl=ro&sa=X&ved=2ahUKEwiEgpqMndfoAhULHcAKHdFqBO04ChDoATAAegQICxAq#v=onepage&q=tularemia%20Russia%202005%20biological%20weapon&f=false, retrieved on 02.04.2020.

[32] Kristy Young Johnson, Paul Matthew Nolan, *op.cit.*, p. 98.

[33] *Botulinum Toxin (Botulism*), UPMC Center for Health Security, 2014, 26.02.2014, http://www.centerforhealthsecurity.org/our-work/publications/botulinum-toxin-botulism-fact-sheet, retrieved on 02.04.2020.

[34] *Botulinum Toxin (Botulism), op. cit.*

[35] Raluca Băjenaru, *Prof. Dr. Ioan Cantacuzino, fondatorul școlii române de microbiologie*, 08.02.2012, https://medicaacademica.ro/prof-dr-ioan-cantacuzino-fondatorul-scolii-romane-de-microbiologie/, retrieved on 01.04.2020.

[36] Michael Pollan, *The Omnivore's Dilemma: A Natural History of Four Meals*, Penguin Books; First edition, 11 April 2006.

[37] Alex Koppelman, *What's Wrong with Our Food?,* Salon, 07.12.2006, http://www.salon.com/news/feature/2006/12/07/pollan_bad_food/, retrieved on 10.03.2020.

infections caused by the consumption of spinach cans infected with Salmonella, 2008 was the year of the tomatoes infested with the same entero-bacillus, stating that *"80% of the beef in the USA comes from the farms owned by four companies, other two process lettuce leaves, and 30% of the milk is processed by a single company"*. This way, a pathogen insinuated in the line of production of the *fast food*, semi-prepared or canned food can reach, without any difficulty, to any region of the globe. Subsequently, cases of severe botulism toxin infections triggered by the consumption of insufficiently cooked chili cans (the case of Castleberry's Food Company in 2007) or epidemic alerts on certain foods (cucumbers contaminated with E-coli bacteria in 2011) confirm the American journalist's fears.

Medical branches such as major surgery, oncological chemotherapy, organ transplantation, therapies for degenerative diseases have begun to face increasing bacterial resistance to antibiotics, a consequence of drug abuse.

The global pandemic of antibiotic resistance is another topic of concern to public health professionals. Medical branches such as major surgery, oncological chemotherapy, organ transplantation, therapies for degenerative diseases have begun to face increasing bacterial resistance to antibiotics, a consequence of drug abuse. Under these conditions, the rate of antibiotics obsolescence has far exceeded the discovery rate of new and effective ones. It is notorious for the worldwide resurgence of multidrug-resistant tuberculosis and the emergence of methicillin-resistant staphylococci (synthetic penicillin, the antibiotic of choice in systemic staphylococcal infections) in the 1990s as a result of antibiotic abuse. Generally, if an infection is detected before germs enter the bloodstream, it is easily resolvable medicinally through targeted antibiotic therapy. But, if bacteraemia/sepsis has occurred, the only antibiotics that can destroy the germs are the reserve ones, so called, as they are the last option to treat the infection. The problem is extremely serious, because the appearance of bacterial strains with multiple resistance is faster than the rate of discovery of new antibiotics, being a matter of time until staphylococci or other lethal bacteria appear through the acquired resistance to any type of antibiotic[38].

[38] *Antimicrobial Resistance*, 15.02.2018, WHO, https://www.who.int/news-room/fact-sheets/detail/antimicrobial-resistance, retrieved on 03.04.2020.

c) Protozoa

Malaria

Malaria is, without a doubt, one of the great killers of mankind. In 2018, malaria affected 228 million people, of whom over 405,000 died [39]. It is endemic to tropical and subtropical regions of Africa, Asia, Central and South America, where the humid and warm environment, to which are added the puddles, swamps and sewer systems clogged in large urban areas, create ideal conditions for the development of anopheles mosquitoes. The cause of this blood parasitosis is a protozoan, *Plasmodium malariae*, with its four subtypes, of which the most common are *Plasmodiumvivax* and *Plasmodiumfalciparum*. In some regions of sub-Saharan Africa, the prevalence of the disease exceeds 90% of the population. In addition to the loss of life, malaria also has major economic impact because:

- the incapacity to work because of recurrent fever episodes;
- the cost of treatment and hospitalisation;
- the frequency of genetic anomalies such as sickle cell anaemia or thalassemia, generated by the plasmodium infection;
- the decrease in tourist and associated economic activities etc.

It is considered that the economic impact of malaria on Africa exceeds $ 12 billion annually[40], and in high-prevalence countries it can cost over 40% of healthcare spending. Mention should be made that, in Africa, HIV infection, tuberculosis and digestive infections are endemic, these debilitating diseases favouring the recurrence of malaria attacks. Practically, in the future, against the background of the worsening economic crisis and the deterioration of the living conditions in the above-mentioned regions, we can expect an increase in the number of victims of this scourge and an additional economic burden on the affected states.

[39] *World Malaria Report 2019*, World Health Organisation, 4 December 2019, https://www.who.int/publications-detail/world-malaria-report-2019, retrieved on 01.04.2020.

[40] B.M. Greenwood, K. Bojang, C.J. Whitty, G.A. Targett, *Malaria,* Lancet 365: 1487-1498, 2005, doi:10.1016/S0140-6736(05)66420-3. PMID 15850634, https://www.ncbi.nlm.nih.gov/pubmed/15850634, retrieved on 02.04.2020.

Insects used as vectors for the disease transmission. In 2008, American entomologist Jeffrey A. Lockwood published a book called *Six-Legged Soldiers: Using Insects as Weapons of War*[41], stating, as the title suggests, that insects are exemplary soldiers that can reach unnoticed the enemy lines and easily transmit lethal maladies. Such an example of lethal malaria transmitted by insects is *Rift Valley Fever*, named after the valley having the same name in Kenya. There, in the east of Africa, in 1931, an unusual epidemic broke out, killing people as well as animals. Subsequently, microbiologists identified the pathogenic agent as a virus transmitted through the direct contact with infected organic fluids or through mosquito bites. This zoonosis can have different forms of manifestation, meningo-encephalitic, haemorrhagic or ocular and, untreated, results in the death of the infected person. Another example is represented by the *Yellow* (liver) *Fever* and *Dengue Fever* viruses, transmitted through the bite of Aedes mosquito. In this context, Professor Lockwood argued that terrorist groups can easily launch a bioterrorist attack using infected insects transported in suitcases that can be introduced, without problems, by terrorists in the territory of the target states, declaring that *"it would be much easier for terrorists to use insects than to develop a nuclear or chemical weapon, as the raw material is in the backyard"*[42]. Lockwood's statements are as serious and logical as possible. It is enough to imagine what would happen if infected Aedes mosquitos were released in a region where the population was not immunised? There would be a huge wave of illness and death, knowing that there is no cure for any of these diseases. Just as the reintroduction of anopheles mosquitos in a region such as the Danube Delta, where such insects existed in the past, would create a very serious epidemiological situation.

Insects are exemplary soldiers that can reach unnoticed the enemy lines and easily transmit lethal maladies.

Last but not least, we should mention ticks, the vectors of Lyme disease. The topic of the military instrumentalisation of ticks resurfaced

[41] Jeffrey A. Lockwood, *Six-Legged Soldiers: Using Insects as Weapons of War*, Oxford University Press, USA, 10 October 2008.

[42] Stephen Adams, *Terrorists Could Use Insect Based Biological Weapon*, *The Telegraph*, 05.01.2009, https://www.telegraph.co.uk/news/earth/wildlife/4123782/Terrorists-could-use-insect-based-biological-weapon.html, retrieved on 02.04.2020.

in the US mass media in 2019, when the US Congress, following an amendment proposed by a New Jersey Republican Congressman, Chris Smith, required an investigation to establish if it was a link between Lyme disease and an alleged Pentagon military experiment. Smith argued the amendment saying that he was inspired by *"a series of books and articles suggesting that important research has been conducted in important US Government facilities, included Fort Detrick, Maryland and Plum Island, New York, to transform ticks and… insects into biological weapons"*[43]. One of the books Smith referred to was *Bitten: The Secret History of Lyme Disease and Biological Weapons*[44], written by Kris Newby, researcher at Stanford University, he himself suffering from Lyme. In the mentioned book, it is stated that American entomologist Willy Burgdorfer (1925-2014), who discovered the disease etiologic agent, *Borrelia burgdorferi* spirochete, would have said that the Lyme epidemics, which affected the US population in the 1960s, could have been a failed military experiment. Moreover, Newby says, Willy Burgdorfer, former researcher in military biotechnologies for the US armed forces, would have stated that he had the mission to grow fleas, ticks, mosquitoes and other blood-sucking insects that he infected with human pathogens. The mentioned military programme had its roots in Nazi Germany, when Dr Erich Traub (1906-1985), who was allegedly involved in military research related to *foot-and-mouth disease, Rinderpesta, pseudorabies, intestinal virus enterovirus 71 and Borrelia*[45]. Traub was supposed to be the chief of *Insel Riems*, a secret Nazi laboratory in the Baltic region, where he had the mission to produce biological weapons meant to destroy the USSR livestock[46]. Arriving in the United States of America after the war, Traub worked as a researcher in the laboratory in Fort Detrick, Frederick, Maryland.

[43] Julian Borger, *House Orders Pentagon to Review If It Exposed Americans to Weaponised Ticks*, *The Guardian*, 16.07.2019, https://www.theguardian.com/us-news/2019/jul/16/pentagon-review-weaponised-ticks-lyme-disease, retrieved on 03.04.2020.

[44] Kris Newby, *Bitten: The Secret History of Lyme Disease and Biological Weapons*, Harper Wave; 1st edition, 14 May 2019.

[45] Karl Grossman, *Lyme Disease and Biowarfare*, Counter Punch, 14.08.2019, https://www.counterpunch.org/2019/08/14/lyme-disease-and-biowarfare/, retrieved on 03.04.2020.

[46] *Ibidem*.

Lyme disease, caused by the bite of a tick infected with *Borrelia burgdorferi*, is known for mobile erythema, accompanied by fever, facial paralysis, arthritis, intermittent pain in tendons, muscles, joints and bones, inflammation of the brain and spinal cord, severe headache and neck stiffness, which eventually leads to death.

INSTEAD OF CONCLUSIONS

Unfortunately, the pandemic and bioterrorist dangers have been constantly placed second in the concerns of policymakers, as evidenced by the way in which the world's states managed the situation in the first months after the outbreak of the current coronavirus pandemics. However, the devastating, multisectoral effects of this pandemics at the state level have demonstrated, once more, that the microbial agent may be the *"David"* that can bring down the *"Goliath".*

In the case of the natural mutation of the pathogen, pandemic effects can be cataclysmic, because genomic *"novelty"* brings about unusual pathogenicity and virulence, treatments that no longer work, panic, overloading the medical system, shutting down the economy, producing many human or animal victims.

In the case of a biological weapon, as the producer must also have an antidote, in order not to destroy his own army/people, the situation is easier to manage, the strains having a limited *"shelf life"* to allow the invasion of the biologically attacked territory.

In both cases, the knowledge of the pathogens, the understanding of their mode of action and, especially, proper preparation and organisation of the means of counteracting and containing the epidemic outbreaks can save lives, jobs, individual freedoms, crops, livestock etc.

Lyme disease, caused by the bite of a tick infected with Borrelia burgdorferi, is known for mobile erythema, accompanied by fever, facial paralysis, arthritis, intermittent pain in tendons, muscles, joints and bones, inflammation of the brain and spinal cord, severe headache and neck stiffness, which eventually leads to death.

BIBLIOGRAPHY:

1. ***, *A Study of The 2001 Anthrax Terror Attacks and the History of Biological Warfare,* 01.04.2015, https://www.fasebj.org/doi/abs/10.1096/fasebj.29.1_supplement.735.3
2. ***, *Antimicrobial Resistance*, 15.02.2018, WHO, https://www.who.int/news-room/fact-sheets/detail/antimicrobial-resistance

3. ***, *Biological Weapons*, World Health Organisation, https://www.who.int/health-topics/biological-weapons#tab=tab_1
4. ***, *Botulinum Toxin (Botulism*), UPMC Center for Health Security, 2014, 26.02.2014, http://www.centerforhealthsecurity.org/our-work/publications/botulinum-toxin-botulism-fact-sheet
5. ***, *Emerging Pandemic Threat And Its Pharmacological Intervention*, *International Journal of Health Sciences*, 2007, July, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3068632/
6. ***, *Feature: Colleagues and Patients Honor Doctor Killed by SARS (2),* http://www.highbeam.com/doc/1P2-13415220.html
7. ***, *Mind the Deadly Gaps: Health Care Worker Shortages in Southern Africa Causing Fatal Delays in Bringing AIDS Care to Those in Urgent Need*, https://www.internationalbudget.org/wp-content/uploads/2011/04/newsletter46.pdf
8. ***, *OMS atrage atenția asupra riscului unei pandemii de gripă*, Rompres, 17.10.2007, http://www.romedic.ro/stiri-medicale/Stiri_generale_0341/OMS_atrage_atentia_asupra_riscului_unei_pandemii_de_gripa_04178.html
9. ***, *Nipah Virus Infection,* WHO, https://www.who.int/csr/disease/nipah/en/
10. ***, *Rice-Detailed Study of Diseases*, http://www.ikisan.com/links/ap_riceDetailedStudyofDiseases.shtml
11. ***, *World Malaria Report 2019*, World Health Organisation, 4 December 2019, https://www.who.int/publications-detail/world-malaria-report-2019
12. Stephen Adams, *Terrorists Could Use Insect Based Biological Weapon*, *The Telegraph*, 05.01.2009, https://www.telegraph.co.uk/news/earth/wildlife/4123782/Terrorists-could-use-insect-based-biological-weapon.html
13. Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World-Told from Inside by the Man Who Ran It*, Delta; Reprint edition, 11 April 2000.
14. Raluca Băjenaru, *Prof. Dr. Ioan Cantacuzino, fondatorul școlii române de microbiologie*, 08.02.2012, https://medicaacademica.ro/prof-dr-ioan-cantacuzino-fondatorul-scolii-romane-de-microbiologie/
15. Julian Borger, *House Orders Pentagon to Review If It Exposed Americans to Weaponised Ticks*, *The Guardian*, 16.07.2019, https://www.theguardian.com/us-news/2019/jul/16/pentagon-review-weaponised-ticks-lyme-disease

16. L. Borio, T. Inglesby, C.J. Peters et al, *Haemorrhagic Fever Viruses as Biological Weapons: Medical and Public Health Management*, 8 May 2002, https://www.ncbi.nlm.nih.gov/pubmed/11988060
17. Anthony P. Cardile, Clinton K. Murray, Christopher T. Littell, Neel J. Shah, Matthew N. Fandre, Dennis C. Drinkwater, Brian P. Markelz, Todd J. Vento, *Monitoring Exposure to Ebola and Health of U.S. Military Personnel Deployed in Support of Ebola Control Efforts – Liberia*, 25 October 2014-27 February 2015, Morbidity and Mortality Weekly Report (MMWR), Centers for Disease Control and Prevention, 03.07.2015, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6425a2.html
18. C. Chi, Q. Sun, S. Wang, Z. Zhang, X. Li, C.J. Cardona, Y. Jin, Z. Xing, *Robust Antiviral Responses to Enterovirus 71 Infection in Human Intestinal Epithelial Cells*, 16 May 2013, US National Library of Medicine National Institutes of Health, https://www.ncbi.nlm.nih.gov/pubmed/23685430
19. Eric Croddy, James J. Wirtz, *Weapons of Mass Destruction: Chemical and Biological Weapons*, ABC CLIO, 2005.
20. Bruce Dorminey, *Ebola As ISIS Bio-Weapon?, Forbes*, 05.10.2014, http://www.forbes.com/sites/brucedorminey/2014/10/05/ebola-as-isis-bio-weapon/
21. Karl Grossman, *Lyme Disease and Biowarfare*, *Counter Punch*, 14.08.2019, https://www.counterpunch.org/2019/08/14/lyme-disease-and-biowarfare/
22. Kristy Young Johnson, Paul Matthew Nolan, *Biological Weapons: Recognizing, Understanding, and Responding to the Threat*, Hoboken, NJ: Wiley, 2016, https://books.google.ro/books?id=O4ebCgAAQBAJ&pg=PA98&lpg=PA98&dq=tularemia+Russia+2005+biological+weapon&source=bl&ots=d90NA_Zxoc&sig=ACfU3U3M16f5YjFVnmHFhqwaNfJv_hUHjQ&hl=ro&sa=X&ved=2ahUKEwiEgpqMndfoAhULHcAKHdFqBO04ChDoATAAegQICxAq#v=onepage&q=tularemia%20Russia%202005%20biological%20weapon&f=false
23. Patrick J. Kiger, *Did Colonists Give Infected Blankets to Native Americans as Biological Warfare?*, *History*, 25.11.2019, https://www.history.com/news/colonists-native-americans-smallpox-blankets
24. Alex Koppelman, *What's Wrong with Our Food?, Salon*, 07.12.2006, http://www.salon.com/news/feature/2006/12/07/pollan_bad_food/
25. Jeffrey A. Lockwood, *Six-Legged Soldiers: Using Insects as Weapons of War*, Oxford University Press, USA, 10 October 2008.

26. Kris Newby, *Bitten: The Secret History of Lyme Disease and Biological Weapons*, Harper Wave; 1st edition, 14 May 2019.
27. Michael Pollan, *The Omnivore's Dilemma: A Natural History of Four Meals*, Penguin Books; 1st edition, 11 April 2006.
28. Alba Iulia Catrinel Popescu, *Jucătorul din umbră*, Editura Militară, București, 2016.
29. Alexandra Șandru, *Pericolul aviar: Crezi ca ne vom confrunta cu o pandemie? (poll),* ziare.com, 29.11.2007, http://www.ziare.com/social/capitala/pericolul-aviar-crezi-ca-ne-vom-confrunta-cu-o-pandemie-sondaj-185674.

SECURITY PROSPECTS – A SOURCE FOR ROMANIAN MILITARY THINKING –

Lecturer Răzvan GRIGORAȘ, PhD
"Carol I" National Defence University, Bucharest

In this article, we address the need for anticipating the future as a way to understand the main changes that could influence national security. The main contribution of this paper is the identification of five tendencies of the future and the analysis of their impact over Romanian military thinking. The purpose of this paper was attained through the analysis of trends and factors – a highly appreciated method for implementing change and development in organisations. In this respect, the main conclusion of this article is that anticipation becomes a milestone for Romanian military thinking. This point makes possible the securitisation of Romania, enabling the Romanian Armed Forces to adapt and to change.

Keywords: strategic prospects, the UN, security foresight, Armed Forces future, cyber security.

I was happy, honoured and proud to receive the "*General Ștefan Fălcoianu*" Award given by the *Romanian Military Thinking* Journal. I wish to thank the Defence Staff and the distinguished evaluators for their trust in the *Security Foresight* project.

INTRODUCTION ON FUTURE APPROACHES

Knowing the future is an old legacy that Glenn[1] considers it under-researched. Unlike the present or the past (which is known through one's experience or memories), the future cannot appeal to certainties. In fact, checking the anticipated results can only be achieved by time passing. For this reason, the idea of anticipation was confined throughout the ages in the sphere of the mystical and the mythical, the scientific element generally missing from the equation.

One of the coherent approaches that emerged the scientific perspective of anticipation belongs to Bertrand De Jouvenel[2]. He introduced the concept of *"possible futures"* – essentially future states that start from a unique situation and prolong to a cone of possibilities. The anticipation methodologies developed later on the basis of this concept.

Bertrand De Jouvenel introduced the concept of "possible futures" – essentially future states that start from a unique situation and prolong to a cone of possibilities. The anticipation methodologies developed later on the basis of this concept.

Today, there are two scientific approaches that sum up the efforts in the field. The first approach – namely prospective studies – summarises the efforts of Glenn[3] and Popper[4]. They consider that anticipation has the purpose of exploring possible futures in order to wisely adopt decisions. The value of this approach consists more in opening minds and less in describing the accuracy of the method.

The second approach – namely foresight – appears in the research of Steenbergen[5] and Gold and Hines[6]. They consider that anticipation

1 J.C. Glenn, *Futures Research Methodology Version 3.0.*, Millennium Project, Washington DC, 2014.
2 B.d. Jouvenel, *L'art de la conjecture*, Ed. du Rocher, Monaco, 1964.
3 J.C. Glenn, *op. cit.*
4 R. Popper, *Foresight Methodology*, 2008, in L. Georghiou, J. Cassingena, M. Keenan, I. Miles and R. Popper (eds.), *The Handbook of Technology Foresight*, Edward Elgar, Cheltenham, 2008, pp. 44-88.
5 B. Steenbergen, *Scenarios As a Powerful Tool for Public Policy*, in *Proceedings of the Prague Workshop on Futures Studies Methodology*, 2005.
6 J. Gold, A. Hines, *An Organizational Futurist Role for Integrating Foresight into Corporations. Technological Forecasting and Social Change*, 2014, DOI: 101. 10.1016/j.techfore.2014.04.003.

needs to better concentrate on planning and on the accuracy of the measuring instruments.

The two approaches have conceived various research styles, mostly at the crossroad between prospective studies and foresight[7]. Studying the future of security and defence was not an important subject for the scientific community. That happened because the anticipation in security and defence was more like a practitioners' topic. This is also the situation for the Romanian military thinking, where the priorities concerned planning military actions in conjunction to the anticipation of the enemy courses of action.

TENDENCIES OF 2050

This paper analyses some strategic prospective products in the field of security and defence (the first scientific approach) and how they can be used by Romanian military practitioners to create a solid strategic posture of Romania in 2050.

This paper analyses some strategic prospective products in the field of security and defence (the first scientific approach) and how they can be used by Romanian military practitioners to create a solid strategic posture of Romania in 2050. In this article, we present the main factors that can influence the future of national security and defence[8].

Scientific literature abounds in analyses of this type, like Sandschneider[9], Al Gore[10], National Intelligence Council[11], UK Ministry of National Defence[12]. Having in mind those papers, we selected five key-factors that will determine the Romanian military thinking to react.

[7] We must mention here the efforts made by Godet, who applies strategic prospect in the field of planning: M. Godet, *The Art of Scenarios and Strategic Planning: Tools and Pitfalls*, in *Technological Forecasting and Social Change*, 65, 3-22, 2000) and those of Georghiou, who focuses on the social-economic dimension of foresight: L. Georghiou, *Third Generation Foresight: Integrating the Socio-economic Dimension*, in *Technology Foresight – The Approach to and Potential for New Technology Foresight, Conference proceedings, NISTEP Research Material 77*, 2001). Other efforts were made by E. Masini, who, in 1983, was thinking about the need to use the prospect also for the transfer of knowledge to planning (E. Masini, *Visions of Desirable Societies*, Oxford, Pergamon Press, 1983).

[8] In specialised literature, the analysis of determining factors comes under many forms, among which the analysis of trends, drivers, weak signals and *black swan*-type events. For more details, see European Foresight Platform, http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/, retrieved on 12 February 2020.

[9] E. Sandschneider, *Drivers of Global Change What Happens When Digital Disruption Meets Geopolitics?*, in *Richard C. Holbrooke Forum*, June 2017.

[10] Al Gore, *The Future: Six Drivers of Global Change,* New York, Random House, ed. 2013.

[11] ***, National Intelligence Council, *Global Trends 2030: Alternative Worlds*, Washington D.C., 2012.

[12] ***, UK Ministry of Defence, *Global Strategic Trends: The Future Starts Today*, London 2018.

These factors are as follows: *(1) shaping a post-petroleum society, (2) tackling pollution and water stress areas, (3) identifying disruptive technologies and tackling cyber space, (4) reformation of UN Security Council, and (5) redefining the global system of alliances*.

ROMANIAN MILITARY THINKING

(1) Shaping a post-petroleum society

The post-petroleum society solves two major problems of our world: (1) controlling energy consumption and (2) reducing pollution and global warming. These two elements are interdependent, and their boundaries often overlap, making their separate analysis difficult.

Many studies contradict themselves in numbers and create inconsistency among decision-makers when analysing energy consumption. For example, GST suggests the probable growth of Global Energy Consumption – up to 60% by 2050[13]. *International Futures* proposes a scenario – orientated perspective[14]. Thus, the overall energy consumption of 2050 may decrease by up to 30%, but may also increase by up to 60%, as shown in *figure 1*. Those differences are not at all encouraging. This is a consequence of two factors with adverse effects: (1) development of service-based economy to the detriment of industries and (2) implementation of the *Internet of Things (IOT)* concept. The first factor decreases energy consumption, shifting its pressure to China, and the second increases consumption, based on the availability of certain devices in the cloud.

There are five key factors that will determine the Romanian military thinking. These are: shaping a post-petroleum society, tackling pollution and water stress areas, identifying disruptive technologies and tackling cyber space, reformation of UN Security Council, and redefining the global system of alliances.

However, some certainties do appear. Firstly, the reduction of energy consumption can only be achieved from an *environmental perspective*. Secondly, consumption will certainly be influenced by resource scarcity. Therefore, the vector of controlling energy consumption is determined by the protection of the environment and renewable energy. This type of society is called the post-petroleum company. It becomes a mobile of the world economic activity. We believe that the emergence of the post-petroleum society is inherent. In contrast, the exact date of occurrence remains questionable, probably after 2050.

[13] *Ibid*.

[14] *International Futures*, 2020.

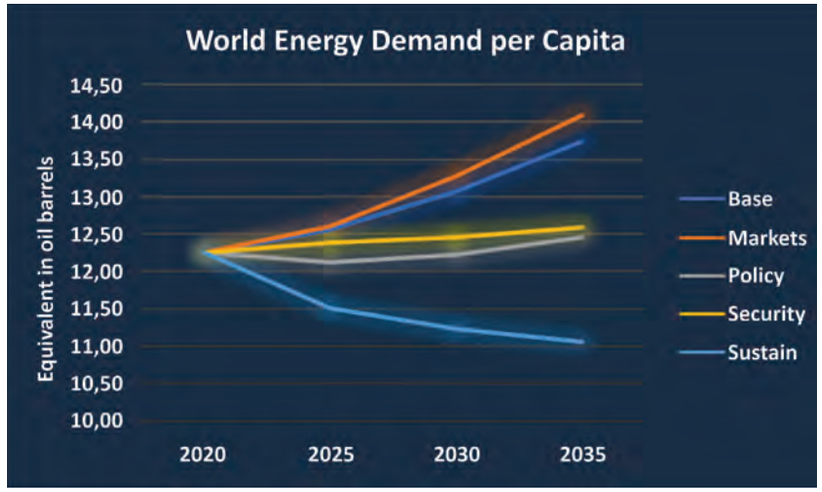

Figure 1: World Energy Demand per Capita[15]

* The Base Scenario takes into account continuing the present policies. The Markets Scenario accentuates the economic measures, the Policy the impact of public policies, the Security the impact of national securitisation and Sustain Scenario the implementation of ecological policies.

According to IHS Global Insight estimates from 2013, shale gas will represent 60% of the US market by 2035. This estimated growth will be accompanied by an investment process that will total over $ 1.9 trillion and will create over 1.6 million jobs until 2035.

This is primarily due to the occurrence of hydraulic fracturing and shale gas exploitation. According to IHS Global Insight estimates from 2013, shale gas will represent 60% of the US market by 2035. This estimated growth will be accompanied by an investment process that will total over $ 1.9 trillion and will create over 1.6 million jobs until 2035.

This factor challenges the Romanian military thinking twofold. First of all, we need a *technological transformation*. This refers to the efficiency of the energy consumption of the military equipment and to the reduction of the carbon footprint of the military actions. Second of all, we need to mitigate risks drawn from *energy security*. This refers to ensuring national energy independence and protecting the critical infrastructures involved in producing or distributing energy.

(2) Tackling pollution and water stress areas

In 2015, the great leaders signed the Paris Agreement – a document that aims to limit the rise of global temperature with 1.5° C by 2050[16].

[15] Credit: *International Futures*, 2020.
[16] *Official Journal of the EU*, 2016.

There is much to be done in this regard. First of all, we have to reduce the use of coal with 50% by 2050 – an ambitious goal. The International Energy Agency predicted in 2017 that by 2050 the world would still rely on fossil fuel energy at over 70% IEA.

The use of freshwater represents a key point. The exploitation and use of freshwater are on the maximum slope worldwide, according to the *Global Strategic Trends: The Future Starts Today*[17] report estimates from 2017. By 2050, we anticipate massive increases in exploiting freshwater (with 1.5 trillion m³ more water than in 2010). Under these conditions, **more than half of the world's population** will not have access to freshwater in 2050.

In Romania, the tendency of using freshwater is difficult to identify. International Futures scenarios tend to identify a turning point in 2040 that will need to be supported by a well-structured ecological policy, as shown in the *figure 2*. According to NIC estimates, Romania will have some severe stress related areas of access to water.

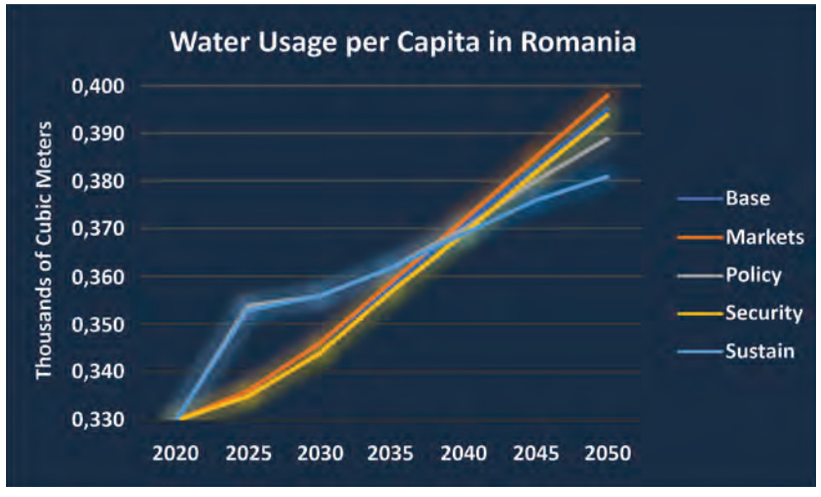

Figure 2: Water Usage per Capita in Romania[18].

* The Base Scenario takes into account continuing the present policies. The Markets Scenario accentuates the economic measures, the Policy the impact of public policies, the Security the impact of national securitisation and Sustain Scenario the implementation of ecological policies.

In Romania, the tendency of using freshwater is difficult to identify. International Futures scenarios tend to identify a turning point in 2040 that will need to be supported by a well-structured ecological policy.

[17] ***, UK Ministry of Defence, *op. cit.*, pp. 17-18.
[18] Credit: International Futures, 2020.

This factor challenges the Romanian military thinking as to ensure that the civil population and military forces have access to freshwater. Downsizing the carbon footprint will become a sensitive issue in 2050 press releases. Never the less, **the stress related areas of access to water** could lead to social revolts and attempts to force its redistribution.

(3) Identifying disruptive technologies and tackling cyber space

Modern technologies and their impact on military actions establish major research themes. Authors like M.L. Cummings[19], Stephan de Spiegeleire et al[20] and Panwar[21] describe the possibilities of using artificial intelligence (AI) in the military field. Some important states – such as the US – intend to militarise the cloud[22]. Last but not least, the impact of IoT on military conflicts becomes a key point in ensuring initiative and freedom of action of forces, as Tonin[23] notes.

Modern technologies and their impact on military actions establish major research themes. Authors like M.L. Cummings, Stephan de Spiegeleire et al and Panwar describe the possibilities of using artificial intelligence (AI) in the military field.

RAND Europe and HCSS have synthesised in a study the main technological issues of our day that can influence the endowment of forces. The themes are (1) the sensorisation and expansion of networks; (2) machine learning and artificial intelligence; (3) globalisation of technology; (4) space as an operating environment; (5) human development; and (6) renewable energy and energy weapons[24].

Today's practice illustrates another major topic: cybersecurity and cybercrime. In 2016, some North Korean actors staged a cyberrobbery that damaged the Bank of Bangladesh with $81 million[25]. In the same year, North Koreans launched the WannaCry ransomware that produced

[19] M.L. Cummings, *Artificial Intelligence and the Future of Warfare*, The Royal Institute of International Affairs, Chatham House, 2017.
[20] S. de Spiegeleire et al., *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers*, The Hague Centre for Strategic Studies (HCSS), 2017.
[21] R.S. Panwar, *AI in Military Operations*, IDSA Strategic Comments, www.idsa.in, 2018, retrieved on 12 February 2020.
[22] ***, US Army, *Army Cloud Computing Strategy*, 2015.
[23] M. Tonin, *The Internet Of Things: Promises and Perils of a Disruptive Technology,* https://www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis, retrieved on 10.02.2020.
[24] *European Defence Matters*, 2017.
[25] D.R. Coats, *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, United Stated Army War College, 2018.

dramatic effects worldwide[26]. In 2017, the US National Cybersecurity and Communications Integration Center (NCCIC) has disclosed publicly that NotPetya malware shut off the local electricity during actions of the Russian Federation in Ukraine. **NotPetya has managed also to stop the functioning of the Chernobyl Nuclear Power Plant monitoring system in addition to the damages of over 10 billion dollars**[27].

On these premises, it is very difficult to anticipate the technological developments that influence military thinking in 2050. **However, we can do some estimation.** One of the most important consequences of technical evolutions is that powerful states will be able to use *nuclear-charged weapon systems* in space by 2050, which will lead to the definition of a new operational space. A second estimation concerns the quality of data and information. GST believes that, as the amount of information will expand, especially in cyberspace, it will be harder to differentiate between truth and fake news[28]. Thus, who will have access to information and data directly from the source, will be stronger. We expect that by 2050, some non-state actors to have access to high-resolution satellite images of the Globe, fundamentally influencing the balance of military confrontations. Certain states and non-state entities have already developed algorithms for civilian population analysis. We expected that these to be used in the planning of asymmetric actions by non-state actors by 2050. It is slightly unclear how the Romanian military thinking will manage to tackle these issues.

One of the most important consequences of technical evolutions is that powerful states will be able to use nuclear-charged weapon systems in space by 2050, which will lead to the definition of a new operational space.

However, the main risk-generating factor in 2050 will be cybercrime. Some authors consider the ability to control cyber space as the future dominant form of power of actors of any kind. Future cyber-actions will be able to create effects on critical infrastructures, industrial facilities and may stop access to public services, **especially for military forces engaged conducted in military actions**. According to GST this will require

[26] *Strategic Cyberspace Operations Guide*, 2018.
[27] M. Scott et al., *Cyberattack Hits Ukraine Then Spreads Internationally*, *New York Times*, 26 June 2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html, retrieved on 10.02.2020.
[28] ***, UK Ministry of Defence, *op. cit.*, pp. 129-137.

the development of a legislative and action framework that is more adequate to protect against cyberattacks[29].

(4) Expansion of the UN Security Council

United Nations (UN) is – according to previous examples in history – the organisation that aims to preserve the status quo mentioned by the treaties following a war (in this case, the Second World War). The UN has managed to maintain its integrity and to remain an important player in world security, presenting its philosophy of peace building. The international practice and the researchers in the field question the success of the organisation due to its institutional capacity for reform and transformation, especially related to Security Council. In essence, the project of the UN Security Council remained partially anchored in the situation of 1945. Since its first meeting in 1952, the membership of the permanent members has remained unchanged (the five winning states of the war). The number of non-permanent members increased from six members to ten members elected for a two-year term. Therefore, the stakes of the reforms are aimed at increasing the portfolio of the permanent members as they have the right to veto. There are several interest groups promoting reform. According to the Ministry of Foreign Affairs, we can identify a number of four groups of states interested in the reform process[30]. They are listed in *table 1*.

The UN has managed to maintain its integrity and to remain an important player in world security, presenting its philosophy of peace building.

The group	Total number	Supplementary permanent members	Supplementary non-permanent members
G4 Germany, Brazil, Japan and India	25	*Plus 6 members:* 2 African states 2 Asian state 1 Latin America state 1 Western Europe State	*Plus 4 members:* 1 African state 1 Asian state 1 SE European state 1 Latin America state

[29] *Ibid*.

[30] The four groups were outlined according to the official data of the Ministry of Foreign Affairs, available in the article *Reforma Consiliului de Securitate ONU*, vezi https://www.mae.ro/node/1589, retrieved on 12 February 2020.

The group	Total number	Supplementary permanent members	Supplementary non-permanent members
Unity for Consensus Italy, Argentina, Pakistan, Mexico	35	Total remains the same.	*Plus 20 members:* 6 African states 5 Asian states 4 Latin America states 3 Western Europe states 2 Se Europe states
African Union (Ezulwini Consensus)	26	*Plus 6 members:* 2 African states 2 Asian state 1 Latin America state 1 Western Europe State	*Plus 5 members:* 2 African states 1 Asian state 1 SE European state 1 Latin America state
Group of the 21	*Promoting only change in procedures.*		

Table 1: Interest groups correlated to revision the UN Security Council[31]

We believe that growing the number of permanent members of the Council may increase the positive perception of international actors about the UN and may limit their revisionist actions. **This factor influences the Romanian military thinking from a fundamental perspective.** The UN Security Council regulates the pulse and intensity of the interventions and determines the global framework for interpreting security. For this reason, the lack of consensus on Security Council reform (especially permanent members) will certainly encourage revisionist attempts to address the international status quo. Therefore, the assurance of national security will be directly affected, by stepping into a new phase that is heading towards conflict.

(5) Redefining the global system of alliances

The global system of alliances ensures the distribution of power between the actors of international relations, being a marker of peace and conflict. The historical experience of two antagonistic blocks of allies is crucial in this regard. Moreover, today's world has outgrown

The global system of alliances ensures the distribution of power between the actors of international relations, being a marker of peace and conflict. The historical experience of two antagonistic blocks of allies is crucial in this regard. Moreover, today's world has outgrown the bipolar paradigm of the Cold War and become multipolar.

[31] Credit: the author.

the bipolar paradigm of the Cold War and become multipolar. Some authors consider multipolarity an intermediate step towards a new bipolarity and examine the growth of China or India in relation to the US[32]. Those authors place China or India in a potential challenger for the US after 2040. For this reason, any alliance system that includes China or India becomes, in turn, a marker of possible conflict. Therefore, by 2050, a balanced distribution of power between the US, China, the Russian Federation, India, Japan and the European Union is desirable. The transformation of the European Union project into a more solid one, with a larger federal substance, becomes a nexus of the 2050s. The cultivation of the exchange of human, material and economic resources represents a bandage for the possible conflictual elements. 2050 brings a *"no go area"* for a possible alliance developed along the axis **China-India-Russian Federation** and a series of *"named area of interest"* regarding the **strengthening of the European Union and the Transatlantic Partnership**. The enlargement of the Alliance and of the European Union is necessary for the foundation of a viable international strategic position of all the countries. The dual foreign policy game of some state actors within these organizations cannot have positive consequences at international level.

Redefining the global system of alliances will definitely cause changes in the extent of the technical endowment, in the procedures but also in the organisation of the Romanian military system. The geographical position of Romania has demonstrated throughout history that the redefinitions of the membership of various alliance systems have not had a positive dynamic contribution on national security.

This factor influences the Romanian military thinking from a fundamental perspective. Redefining the global system of alliances will definitely cause changes in the extent of the technical endowment, in the procedures but also in the organisation of the Romanian military system. The geographical position of Romania has demonstrated throughout history that the redefinitions of the membership of various alliance systems have not had a positive dynamic contribution on national security. From the point of view of the Black Sea exit, Romania

[32] In this respect, we should mention H.P. Pant, *Contemporary Debates in Indian Foreign and Security Policy*, New York: Palgrave Macmillan, 2008. He considers India as a potential challenger for the SUA. Another analysis that must be taken into account is the one conducted by G.J. Ikenberry, *The Future of the Liberal World Order: Internationalism after America*, *Foreign Affairs* 90(3), 2011, http://www.eastlaw.net/wp-content/uploads/2016/09/Future-of-Liberal-world-order-90ForeignAff56.pdf, retrieved on 12 February 2020. He sees China as a potential challenger for the USA. This idea is also embraced by H. Kissinger, in *On China*, The Penguin Press, New York, 2011.

becomes a *sui-generis* state of the North Atlantic Alliance and of the EU. Against the backdrop of Turkey's cryptic game in the region, as well as the actions of the Russian Federation, Romania's road to 2050 must be predictable for the current allies, but even more consistent in terms of a sustainable European project. Defining regional projects (such as B9) only strengthens the strategic position of our country. The military technique will have to keep up with the innovations in scientific research in the Allied community. This will prove unlikely to be achieved at the level of 2050, if European defence initiatives will not gain strength and the EU will not identify concrete ways of providing domestic insurance.

ROMANIAN MILITARY THINKING

CONCLUSIONS ON THE ADAPTATION OF THE ROMANIAN MILITARY THINKING

Essentially, the anticipation represents a mobile through which the Romanian military thinking can create the basis of Romania's securitisation in 2050. Even if we shall define security with other landmarks in 2050, this concept will remain the dome under which citizens manage to make a living, feeling in safety. For this reason, the Romanian Army will have to adapt and find solutions to fulfil its missions.

The Romanian military thinking will have to react and support Romania's energy security. At the same time, it must prepare the military technological adaptation and downsize the carbon footprint of military actions.

This article has presented the main factors that will have an impact on national security in 2050, in order to draw some lessons for the Romanian military thinking. Probably one of the most important issues to tackle with is the transition towards an ecological (post-petroleum) society. This will happen against the increased pollution and the precariousness of fresh water resources. The interactions of the two factors will create the premises for profound changes in Romania, from technological adaptation to adapting the day-to-day life.

The Romanian military thinking will have to react and support Romania's energy security. At the same time, it must prepare the military technological adaptation and downsize the carbon footprint of military actions. The final effect will have a tripartite structure, aimed at (1) ensuring national energy independence, (2) protecting the critical infrastructures involved in the energy production

or distribution process, and (3) preventing social upheavals because of the precariousness of fresh water resources.

From our point of view, technological innovations represent the most disruptive factor to anticipate in the Romanian military thinking. Although innovations will profoundly transform our society, it is not clear at this time when and if they will truly trigger a new **revolution in military affairs**, as the **machine-gun appearance** did, for example.

However, it is certain that, in this very moment, serious steps are being taken to apply a new concept – the Internet of Things – that **can become the engine of this revolution**. Connecting all devices to an integrating platform, based on 5G speeds, will create the foundation for cascading effects, both positive and negative. The major opportunities of the IOT-5G binomial will allow the increased awareness and sensorisation of the modern combat environment. There are also negative effects, including increased vulnerability to cyber-attacks. Considering that some entities have already developed algorithms for civilian population analysis and that they will also have access to detailed maps through various satellite platforms, this will turn them into feared enemies. Therefore, the Romanian military thinking will have to find solutions to cope with the expansion of the networks that will allow the monitoring of all the specific elements of the training environment or the modern battlefield, from individual performances to deepest threats.

The Romanian military thinking will have to find solutions to cope with the expansion of the networks that will allow the monitoring of all the specific elements of the training environment or the modern battlefield, from individual performances to deepest threats.

At the same time, the Romanian military thinking will have to counteract the new **possibilities of designing the force in military actions** (cosmic space, cyber space, air space – with reference to drones and drone swarms). A balance will be needed between military technological investments and the cultivation of a specific alliance system. For this reason, the redefinition of the global system of alliances or the UN Security Council will definitely determine changes in the extent of technical endowment, in the procedures applied in times of crisis but also in the organisation of the Romanian military system. Integrating cyber actions into current operations is one of these changes.

BIBLIOGRAPHY

1. ***, *Paris Agreement*, L 282/4 RO, *Official Journal of EU from* 19.10.2016, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22016A1019(01)&from=RO.
2. ***, *Disruptive Defence Innovations Ahead, European Defence Matters*, no. 17, 2017.
3. ***, *International Futures (IFs) Modeling System*, Frederick S. Pardee Center for International Futures, Josef Korbel School of International Studies, University of Denver, Denver, 2020, http://www.ifs.du.edu/ifs/frm_MainMenu.aspx.
4. ***, Ministry of Defence UK, *Global Strategic Trends: The Future Starts Today*, London, 2018.
5. ***, *Strategic Cyberspace Operations Guide*, United States Army War College, Center for Strategic Leadership, 2018, https://info.publicintelligence.net/USArmy-StrategicCO.pdf.
6. ***, *The Economic and Employment Contributions of Shale Gas in the United States*, IHS Global Insight, www.nic.gov.
7. ***, National Intelligence Council, *Global Trends 2030: Alternative Worlds,* Washington D.C., 2012.
8. ***, US Army, *Army Cloud Computing Strategy*, 2015.
9. K. Bertolucci, *Taxonomy for the Future: Organizing Futures Information into a New Hierarchical Structure*, in *Future Research Quaterly*, 2004.
10. M.L. Cummings, *Artificial Intelligence and the Future of Warfare*, The Royal Institute of International Affairs, Chatham House, 2017.
11. J.C. Glenn, *Futures Research Methodology Version 3.0*, Millennium Project, Washington DC, 2014.
12. G.J. Ikenberry, *The Future of the Liberal World Order: Internationalism After America*, *Foreign Affairs* 90(3), 2011, http://www.eastlaw.net/wp-content/uploads/2016/09/Future-of-Liberal-world-order-90ForeignAff56.pdf.
13. B. d. Jouvenel, *L'art de la conjecture*, Ed. du Rocher, Monaco, 1964.
14. H. Kissinger, *On China*, The Penguin Press, New York, 2011.
15. H.P. Pant, *Contemporary Debates in Indian Foreign and Security Policy*, Palgrave Macmillan, New York, 2008.
16. R.S. Panwar, *AI in Military Operations*, IDSA Strategic Comments, 2018, www.idsa.in.
17. R. Popper, *Foresight Methodology*, 2008, in L. Georghiou, J. Cassingena, M. Keenan, I. Miles și R. Popper (eds.), *The Handbook of Technology Foresight*, Edward Elgar, Cheltenham.
18. Stephan de Spiegeleire, Matthijs Maas, Tim Sweijs, *Artificial Intelligence and The Future of Defense: Strategic Implications for Small and Medium-Sized Force Providers*, The Hague Centre for Strategic Studies (HCSS), 2017.

POSSIBLE SOLUTIONS FOR THE IMPLEMENTATION OF A STRATEGY – THE PLACE OF MARITIME STRATEGY –

Lucian Valeriu SCIPANOV, PhD
"Carol I" National Defense University, Bucharest

The attempt to identify a possible solution for the realisation of a national defense strategy derives from the extrinsic motivation to quantify those national security objectives that find their representation in strategies and doctrines. The national defense strategy contains those directions, corresponding to the national objectives, regarding the manifestation of interests at the national and international levels. The identification of a model that achieves a connection between the ends, the ways of accomplishment and the means necessary to reach the national security objectives, represents a necessary step to the theoretical level of the strategic thinking from which the practical thinking extracts its foundations. The novelty of this approach derives from the intrinsic motivation to promote the opportunity of a maritime strategy and to identify the level of its representativeness within the National Defense Strategy and the Military Strategy. Through this approach, I address the specialists, those who contribute to the development of strategic and doctrinal documents, the master's degree and doctoral students, the student officers, those interested in the mechanism of developing a strategy, to have at hand a possible solution for the realisation of the national defenses strategy, and also to identify the correlation between the component elements (ends-ways-means) and their implications at the level of secondary strategies and doctrines.

Keywords: seecurity strategy, defense strategy, maritime strategy, maritime power, the Ends, Ways & Means model.

INTRODUCTION

The term *strategy*, according to the *Explanatory Dictionary of the Romanian Language*, represents *"a component part of the military art, which deals with the problems of preparation, planning and conducting of war and military operations"*[1].

The term has its origin in Greek, being made up of the terms *stratos* (army) and *agein* (leadership)[2].

In the Greek understanding of the term, *strategos* was called the general, the commander of the army; *stratego*[3] represented the ability to command, to be commander, to be general, along with the derivatives of the term which covered, as a general meaning, the functions of the general or his qualities.

In the Greek understanding of the term, strategos was called the general, the commander of the army; stratego represented the ability to command, to be commander, to be general, along with the derivatives of the term which covered, as a general meaning, the functions of the general or his qualities.

Even though I identified many military connotations of the term, I also came across meanings of the term, which refer to policies, plans and directions of action in different fields of application: game strategies; development strategies; economic strategies, and so on. Thus, in the first instance, I can conclude that strategy represents a systematic, well-grounded plan, through which certain planned objectives are implemented, using the specific means at hand, and that contributes to the fulfillment of the purpose for which it was achieved.

In the national approach, the scientific aspect of the term is mentioned, i.e. strategy represents the *"fighting leadership science"*[4] and – in another approach – I found out that strategy represents *"the art of using all the available means with a view to ensuring success in combat"*[5].

[1] According to dexonline.ro retrieved on 10.02.2020.
[2] According to https://www8.gsb.columbia.edu/articles/ideas-work/von-clausewitz-war-six-lessons-modern-strategist, retrieved on 22.02.2020.
[3] Verb – *strategos*, adjective – *strategikos*, noun – *strategika* (pl.) [A/N].
[4] *Dicționar de neologisme*, Editura Steaua Nordului, 2002.
[5] *Ibid*.

At the political-military level, strategy covers much more than the military side. In different situations, strategy covers the fields of security (security strategy), the field of defense (defense strategy), the military field (military strategy), the maritime field (maritime strategy), and so on.

Strategy was brought into attention by philosophers, leaders, historians, and writers, who gave it different meanings, which in principle covered the need for understanding and using the term. Frederik the Great[6] was one of those who understood the importance of a unified vision of the state leadership and the defense approach from a scientific perspective: *"He who defends everything defends nothing"*[7], representing the acceptance that a defense strategy is a solution on an optimal response regarding the security of the kingdom (Prussia).

"The strategy is the science of war; it outlines the plans, has the general vision and determines the course of the military actions, it is, exactly speaking, the science of the commanding generals".

Clausewitz was the one who best emphasised this aspect, stating that *"strategy is to use war for the purpose of war"*[8], thereby providing a first modern military perspective on the term.

Previous opinions outline the idea that strategy is not only a science, but also an art.

STRATEGY IS SCIENCE AND ART

"The strategy is the science of war; it outlines the plans, has the general vision and determines the course of the military actions, it is, exactly speaking, the science of the commanding generals"[9]. Being a science, the theoretical character of the meaning is emphasised: *"Strategy must study combat in relation to its possible results, as well as with the most important intellectual and moral forces in its use"*[10].

[6] Frederick II or Frederick the Great (1712-1786), King of Prussia, Hohenzollern dynasty [A/N].
[7] Frederick the Great, https://devcentral.f5.com/s/articles/he-who-defends-everything-defends-nothinghellip-right, retrieved on 22.02.2020.
[8] Carl von Clausewitz (1780-1831), translated by Corneliu Soare, *Despre război*, Editura ANTET XX PRESS, p. 72.
[9] Archduke Charles, Duke of Teschen, A. S. I. l'archiduc Charles; translation from German by Antoine Henri Jomini, *Principes de la strategie*, Paris, 1818, *Chapitre premier, Section premiere*, p. 1.
[10] Carl von Clausewitz, *op. cit.*, p. 72.

On the other hand, strategy is an art. *"Strategy is the art of combining preparations for war and the grouping of operations to achieve the aim put forth by war for the armed forces"*[11]. Strategy is an art based on the knowledge of the commander and his intuition, that spark of genius, hard to reach without an experience in weapons.

In this way, practitioners differ from theorists: *"The researcher who, starting from this success of assembly, does not see that harmony, often looks for genius where the latter is absent and cannot exist"*[12].

From the point of view of international relations and national security, Lecturer Edward Mead Earle stated: *"strategy is the art of controling and utilising the resources of a nation, or of a coalition of nations"*[13], an aspect that represents a new scientific approach to the term from a military perspective, with effects on economic security.

On the other hand, Professor Colin Gray mentioned that strategy is the product of the dialogue between politics and the instruments of power; it is a bridge between political goals and military means. *"Often polities decide on policy, then decide on an action, but neglect to tie the two realms together. The purpose of the strategist is to bridge this gap by being well-armed with the General Theory of Strategy"*[14].

The strategist must have an integrated vision, comprehensive of the battlefield, where he will exert his leadership qualities according to a number of factors, internal and external, political and economic, which will influence his approach.

The strategist must have an integrated vision, comprehensive of the battlefield, where he will exert his leadership qualities according to a number of factors, internal and external, political and economic, which will influence his approach. *"The strategist must take into account the state's entire rear area, his own and that of the enemy with all its political and economic potentials"*[15].

"Strategy provides the bridge between military means and political goals"[16], an aspect that finds its foundation in some general laws

"Strategy provides the bridge between military means and political goals", an aspect that finds its foundation in some general laws of the war.

[11] David M. Glantz, Harold S. Orenstein, *The Evolution of Soviet Operational Art, 1927-1991: The Documentary Basis*, Vol. I, Franc Cass London, 1995, p. 6.
[12] Carl von Clausewitz, *op. cit.*, p. 72.
[13] Edward Mead Earle (1894-1954), Professor of security studies, Princeton, *Strategy: Create and Implement the Best Strategy for Your Business*, Harvard Business Review, p. XII.
[14] Colin Gray (1943) – Professor of Oxford and Manchester – strategic studies, Colin Gray, John Baylis, James Wirtz, *Strategy in the Contemporary World*, Oxford University Press, 2019, p. 391.
[15] David M. Glantz, Harold S. Orenstein, *op. cit.*, p. 6.
[16] Colin Gray, *op. cit.*, p. 5.

of the war: *"The law of the dependence of the course, the denomination, the consequences of the war on the quality of public decision acts; The law of the dependence of the armed confrontation on the economic, technical, scientific potential of the states involved; The law of the role of the nation in sustaining the war effort"*[17]; *"The law of the concordance between the political purpose, forces, means, resources and objectives"*[18].

As a partial conclusion, I can point out that *strategy* is the art of leadership (the art of command in general), but one should not minimise the theoretical side, in which strategy is a science. Therefore, strategy represents, beyond the controversy over its nature, a science and an art in equal measure.

If we refer to the strategy of an organisation, this is the way in which the organisation prepares itself for an uncertain future, through which to face the challenges of any kind, through a response identified as a solution.

Having presented these characteristic elements of the term, I think that strategy is the art and science of employing the political, economic, psychological, military and security instruments of a nation in order to meet the political objectives in competition with other actors pursuing their interests. In my opinion, strategy is the subject of a unanimous agreement; it is both art and science, so it is a bridge between theory and practice; strategy is a process, with a much more complex content than the meaning it bears.

Strategy represents the way things should be done; it presents the general path through which the set objectives are achieved. I want to emphasise that strategy is a process in itself and not a goal. If we refer to the strategy of an organisation, this is the way in which the organisation prepares itself for an uncertain future, through which to face the challenges of any kind, through a response identified as a solution.

In my opinion, strategy is manifested by two components, *hard* and *soft*; the hard components are represented by the elements of military

[17] Mircea Mureşan, Costică Ţenu, Lucian Stăncilă, *Corelaţia artei militare cu fenomenul militar contemporan, Curs de artă militară*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2005, pp. 95-100.

[18] Gheorghe Văduva, *Principii ale războiului şi luptei armate – realităţi şi tendinţe*, Universitatea Naţională de Apărare *"Carol I"*, Centrul de Studii Strategice de Apărare şi Securitate, Bucureşti, 2003, p. 4.

power; the soft components are represented by politics, economy, technology, culture, state tradition etc.

Next, I will approach the term from the perspective of security and defense and their influence on the *hard* component (i. e., military power).

To identify at what level of leadership we can develop a strategy, I will call on the levels of the military (i. e., strategic, operational and tactical art).

THE LEVELS OF STRATEGY

From this perspective, the levels of strategy are identified primarily at the political and military levels. The political strategy (called the Grand Strategy[19]), contains all the power tools of the state. Military strategy describes how to employ the military instrument in times of peace, crisis, or war. *"Policy is the ways (methods or patterns) by which strategy reaches its objectives"*[20].

The levels of strategy are identified primarily at the political and military levels. The political strategy (called the Grand Strategy), contains all the power tools of the state. Military strategy describes how to employ the military instrument in times of peace, crisis, or war.

In the military field, strategy has operational and tactical influences. At the operational level, the strategy on the theater of operations describes how to employ the military instrument at regional level, and, at the tactical level, the strategy of the different services describes a specific strategic concept (strategy).

Let us further see in which areas we can identify the opportunity to develop strategies. I identified four levels of strategy manifestation: *The Grand strategy*[21]; *the strategic level*; *the operational level* and *the tactical level*.

The grand strategy represents the level at which the political-military decisions are made; it is determined by whether a country enters the war or not, who the enemies will be, who the allies will be

[19] *"Grand strategy"* (Clausewitz, Liddell Hart, Corbett) refers to the diplomatic and political-military level of the strategy [A/N].

[20] *Strategy: Ends and Means*, p. 39, at https://www.globalsecurity.org/military/library/policy/usmc/mcdp/1-1/mcdp1-1_chap2.pdf, retrieved on 22.02.2020, *"grand strategy"*, "*grand national strategy*" or, currently in the United States, *"national security strategy"*.

[21] Colin Gray, *op. cit.*, pp. 319-321.

and what they want as a result of peace. At this level, it is essential to be able to lead the war, to build alliances, coalitions, partnerships, in order to know from the very beginning which position they want to hold in negotiations (which kind of peace they want).

Therefore, the grand strategy represents the state's war policy. Its purpose is to coordinate and direct all resources of the nation or of a coalition, alliance, union, partnership, in order to achieve the political objective of the war.

The grand strategy represents the state's war policy. Its purpose is to coordinate and direct all resources of the nation or of a coalition, alliance, union, partnership, in order to achieve the political objective of the war.

The USA does not use the term *Grand strategy*, but rather uses the term *national strategy*; the UK uses it, with this meaning: *"an application of national resources to achieve national policy objectives and which involves economic, industrial, political and military components"*[22].

The strategic level aims at the general war management and estimates the forces that will be available; it also distributes the war effort among the different war theaters. The operational level represents the level that aims at reaching the end of the war with the assigned forces. This is the level at which the plans for the employment of land, air and maritime forces are drawn up and the level of employment of these forces stipulated during the campaign.

The tactical level is the place where the opposing forces are physically confronted and where the objectives set by the upper echelon are clear. *"Tout plan strategique doit pouvoir être mis à l'exécution par les mayeurs de la tactique"/"Any strategic plan must be made by the tactical mayors"*[23].

This is the level of execution, of implementation of tasks specific to the objectives specified in the mission. The fulfillment of orders at the tactical level does not require a special mental effort, but it requires knowledge, intuition, experience, will, determination, which are the attributes of a good tactician.

[22] G. Sheffield, G. Till, *The Challenges of High Command: The British Experience,* Palgrave Macmillan, New York, 2003, p. 191.
[23] A. S. I. l'archiduc Charles; translated of Antoine Henri Jomini, *op. cit*., p. 3.

STRATEGIC THINKING AND OPERATIVE THINKING

According to the ones presented, I identified two levels of thinking, i. e., strategic thinking and operative thinking, identifying a substantial delimitation between the upper level of application (strategic level) and the lower level (operational and tactical level). Practically, I differentiated the theoretical level related to the political-military level from the practical level related to the operative-tactical level.

Strategic thinking is achieved in the long term. It is conceptual, reflective-cognitive thinking because it is based on theoretical foundations, laws, principles, the decision being scientifically argued. *"The strategist's weapons are strategic thinking, consistency and coherence"*[24].

Strategic thinking is achieved in the long term. It is conceptual, reflective-cognitive thinking because it is based on theoretical foundations, laws, principles, the decision being scientifically argued. "The strategist's weapons are strategic thinking, consistency and coherence".

Strategic thinking is short-term; it identifies the opportunities, the most appropriate response variants for the hypothetical situation. The dynamics of the action environment involve an adaptation of the strategy to the existing news through unique solutions. Strategic thinking aims at achieving an optimal efficiency ratio. Thus, at this level, strategy has the role of identifying those response variants that are the most appropriate (the ones that are needed), the image of the planners being a general one.

Operational thinking is realised in a shorter term, immediately applicable, in a concrete mode of action. Operational thinking is characterised by routine, actionable experience, heuristics of the operational level commander. It is a dynamic action, an adaptive one because as problems arise, they are solved. Strategic thinking aims to achieve goals through effective solutions that solve problems by all means. Thus, at the operational level, strategy has the role of identifying appropriate solutions (as it should), the image of the planners being a local, limited one.

[24] Kenichi Ohmae (1943-dean UCLA), *The Mind of the Strategist: The Art of Japanese Business,* Paperback, Editura McGraw-Hill Education, 1991, p. 57.

Having in mind the ideas presented up to this point, I can conclude that strategy is a concept in itself because it encompasses a series of descriptive meanings and terms, which coagulate around science and art. So strategy is not a sum of the constituent elements of a system, but rather a concept. I also state that strategy is a process.

STRATEGY AS A PROCESS COMPARED TO STRATEGY AS A CONCEPT

Next, let us look into the dominant features of strategy as a process compared to strategy as a concept.

Strategy as a concept delimits politico-military dependencies; it links politics with military operations, defines political and military analysis criteria, so that an effective strategy must integrate political and military criteria rather than separate them, avoiding thereby the tendency to separate the opinions of civilian and military leaders.

Strategy as a process encompasses a series of interdependent actions, which are carried out on all the levels of manifestation of security: determining the national security objectives; formulating the political strategy; developing of the military strategy; designing the operative strategy (doctrines); formulating the battlefield strategy (tactics).

Strategy as a concept delimits politico-military dependencies; it links politics with military operations, defines political and military analysis criteria, so that an effective strategy must integrate political and military criteria rather than separate them, avoiding thereby the tendency to separate the opinions of civilian and military leaders.

Given the new context of regional security, I consider it is opportune to develop strategies to respond to the globalisation under the conditions of new competitors, challenges and dangers, risks and threats, etc. The competition for resources generates new regional actors, so the old principles need to be adapted to the new security climate. New times, new principles I would say, however, I believe that adaptation is the key to success, so the old principles remain in the spotlight. Why would we need a new strategy? If we look at the security environment, it is defined as multipolar, so the arguments presented above, support the idea of a new strategy.

A possible solution for the realisation of a strategy

„Strategia naţională de apărare a ţării pentru perioada 2015 – 2019 – O Românie puternică în Europa şi în lume" ("The National Defence

Strategy 2015-2019 – A Strong Romania within Europe and the World") was applied between 2015-2019. *"The document facilitates the understanding of how the state – while respecting the fundamental rights and freedoms of the citizen – exerts through its institutions the responsibilities regarding the security of the country and the safety of its citizens"*[25].

Even though the security environment is in a continuous dynamic, the content elements of the strategy remain largely up-to-date. I am certain that the new security threats will be analysed and taken into account in order to define the next strategic directions.

Next, I want to identify a possible solution for the realisation of a strategy, to see in fact what the process itself is, from the institutional approach to its content.

The institutional process of elaborating a national defense strategy begins with a debate at the national level regarding the realisation of a strategy project, following the refinement and optimisation of the content. In this form, it is submitted to the Parliament by the Romanian President, within a maximum of three months from the investiture[26].

A strategy builds on the political and strategic options and decisions of the Romanian Parliament, of the public institutions that have attributions in the field of national security and defense, which must estimate the resources allocated and the necessary means in the long term, in order to offer the possibility of achieving the security and national defense.

The defense strategy includes measures and activities that must be adopted and carried out by the Romanian in order to guarantee the national sovereignty, independence and unity of the state, the territorial integrity of the country and the values of constitutional democracy, with a five-year evaluation horizon. The defense strategy is a product of the national public authorities established by the Romanian Constitution.

A strategy builds on the political and strategic options and decisions of the Romanian Parliament, of the public institutions that have attributions in the field of national security and defense, which must estimate the resources allocated and the necessary means

[25] https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019, retrieved on 25.02.2020.

[26] *Ordonanța nr. 52, (art. 4) din 12 august 1998 privind planificarea apărării naţionale a României/ Ordinance no. 52, (art. 4) of 12 August 1998 regarding the planning of the national defense of Romania*, republished in the *Romania Official Gazette*, Part I, no. 185 of 28 April 2000.

in the long term, in order to offer the possibility of achieving the security and national defense.

THE PROCESS OF DEVELOPING A STRATEGY

Next, let us see specifically what is the process of developing a strategy.

Following the analysis of several strategies at the international level, I identified that in the first stage the national purpose is defined, which is based on values, beliefs and ethics, national interests, to which vision, strategic education, and policies are added.

In the next stage, a strategic level analysis (strategic analysis) is carried out, at the security environment level, which is carried out in four steps, which I will identify and present below.

The analysis model is based on a process of identifying some directions of action. It starts with defining the strategic environment (step I), at the level of the global and internal security environment. In the next step (step II), a careful analysis of the effects of the defined strategic environment on the national security from all points of view is necessary, in relation to the existing strategies of the neighbors.

An evaluation of the strategies of the emerging countries (step III) is needed to identify common interests that are contrary to national interests. After these first three steps, in step IV variants of the national security action directions are determined.

Phase III is the stage of identifying possible directions of action, risks, and threats.

The analysis of the global environment consists of identifying the regional actors, their armed power, the regional interests, trends of the global and regional security environment. This is an analysis process based on a model similar to the one presented above. The competitors, the economic conditions, the effects of globalisation at the region level, the technological development of the neighbors, the international laws that influence regional security are identified.

The analysis of the global environment consists of identifying the regional actors, their armed power, the regional interests, trends of the global and regional security environment. This is an analysis process based on a model similar to the one presented above. The competitors, the economic conditions, the effects of globalisation at the region level, the technological development of the neighbors, the international laws that influence regional security are identified.

The international organisations operating in the area are also identified. This goes equally for regional actors, state or non-state,

exerting a certain influence. Finally, having all the elements presented, in relation to all the variables that influence security, one can identify the risks and threats that can impact on national security.

Generally, the internal security environment is in direct relation with the governing system, which offers the possibility of all the functions of the state regarding the provision of security to manifest in optimal conditions. The analysis of the internal environment consists of identifying the national authorities that have responsibilities for strengthening national security. It identifies the economic conditions, the needs of the society, the dominant social characteristic (the level of social development), the morale of the society, the independence of the media, etc.

The best-known process model for implementing a strategy is the Anglo-Saxon model defined in clear terms by the American school itself: Ends, Ways & Means[27]:

- *ENDs (objectives):* political level and political-military level (grand strategy, national strategy);
- *WAYs (ways):* which can be identified at the level of strategic thinking and operational thinking from a comprehensive perspective (*comprehensive approach*);
- *MEANs (means):* development of capabilities and means; implementation of strategic directions with the help of developed and available means (at the level of operative-tactical thinking).

I believe that the process of elaborating a national strategy can be based on the Objectives-Ways-Means model, in which we identify:

- national objectives *(Ends)*; identified the purposes;
- strategic concept *(Ways)*; identified the path;
- instruments of national power *(Means)*: identified those means that must be developed in order to achieve the goals; identified

The analysis of the internal environment consists of identifying the national authorities that have responsibilities for strengthening national security. It identifies the economic conditions, the needs of the society, the dominant social characteristic (the level of social development), the morale of the society, the independence of the media, etc.

[27] Gregory D. Miller, Chris Rogers, Francis J. H. Park, William F. Owen, and Jeffrey W. Meiser, *On Strategy as Ends, Ways, and Means*, journal of the US Army War College 47(1):125-126, January 2017.

those resources with can be developed the capabilities which we can provide an optimal response, adequate to the security needs of the following years.

This model of strategy development is based on the result of the global and internal analysis. It has enabled me to identify possible directions of strategic action and conduct a strategic analysis from a comprehensive approach.

This approach consists of identifying national interests based on their prioritisation, defining national values and principles, evaluating the identified problems, trends and challenges, risks, and threats, opportunities to manifest national interests on security.

Following is the application of the previously proposed model, which consists of: determining the objectives (ends), elaborating the alternatives (ways), depending on the resources available or necessary (means) to reach the objectives.

Having performed this analysis, one can proceed to the next step, i. e., risk assessment, in the sense of identifying the most vulnerable pillar of the objectives-ways-means model. The result is a well-founded strategic policy recommendation.

This model can be verified by an analysis that takes into account the following criteria: adequacy, acceptability, feasibility, risk assessment. If the strategic directions obtained respond positively to the analysis of the aforementioned criteria, then we have a strategy.

A BRIEF CASE STUDY

Let us check the applicability of the model by analysing the content of the national defense strategy: *The National Defence Strategy 2015-2019 – A Strong Romania within Europe and the World*.

Stage I

Defined purpose: *"A strong Romania within Europe and the World, a state that ensures the security of its citizens wherever they are"*[28].

[28] *The National Defence Strategy 2015-2019 – A Strong Romania within Europe and the World* (*Strategia Naţională de Apărare a Ţării pentru Perioada 2015-2019. O Românie puternică în Europa şi în lume*), The Presidential Administration, București, 2015.

We identify the national values: *"dignity; civic cohesion and affirmation of national identity; constitutional democracy and the rule of law; the state and territorial integrity of Romania"*[29].

We identify the national principles: *"continuity; predictability; legality; proportionality"*[30]. Also, national security interests are defined. We can identify them in the chapter *1.2. Interese naţionale de securitate*[31] :

Stage II

Step I: defining and evaluating the global and internal strategic environment.

In *Chapter II* of strategy, we can identify the *"international security environment assessment"*[32], in which we find a presentation of the global security environment, the security dimension at the Euro-Atlantic level and the regional security environment. This chapter presents the state of the security environment, its evolution, and trends.

In Chapter II of strategy, we can identify the "international security environment assessment", in which we find a presentation of the global security environment, the security dimension at the Euro-Atlantic level and the regional security environment.

Step II: a careful analysis of the effects of the strategic environment on national security is performed.

Step III: evaluation of the strategies of the regional actors, to identify the common interests and those that contradict the national interests.

As a result of this analysis, we can identify the threats, risks, and vulnerabilities to national security presented in *Chapter III*: "*ameninţări, riscuri şi vulnerabilităţi"*[33] *(threats, risks and vulnerabilities).*

After this step, the *Ends* are obtained, which represent the first pillar in the Ends, Ways & Means triptych. We identify the national security objectives *(Ends)*:

- *"strengthening Romania's profile in NATO and the EU through both conceptual and operational contributions;*

[29] *Ibid*.
[30] *Ibid*, p. 7.
[31] *Ibid*, p. 8.
[32] *Ibid*, p. 11.
[33] *Ibid*, pp. 14-16.

- *respecting the fundamental principles and values of the EU;*
- *strengthening the strategic partnership with the USA, including in the economic and commercial field;*
- *ensuring security in the Black Sea;*
- *deepening cooperation with neighboring states and those on the eastern flank;*
- *intensifying regional cooperation including in the field of defense;*
- *supporting the European path of the Rep. Moldova;*
- *promoting political, economic and security interests in regions of strategic relevance for our country"*[34].

The directions of action and the main ways of ensuring national security (Ways) are: "the defense dimension; the public order dimension; the informational dimension, counter-information, and security dimension; the economic and energy dimension; the diplomatic dimension; the crisis management dimension; the educational, health, social and demographic dimension".

Step IV. Defining the directions of action, following the identification of threats, risks, and vulnerabilities, which in fact represent the *Ways*, the second pillar of the triptych *Ends, Ways & Means*. Let us see what are the *Ways* presented in strategy, through which these objectives can be applied. These are presented in *Chapter IV: Direcţii de acţiune şi principalele modalităţi pentru asigurarea securităţii naţionale a României*[35] (*Directions of action and the main ways to ensure the national security of Romania*). If we analyse the content, we can conclude that here are the means, too, which in my opinion are not sufficiently detailed.

The directions of action and the main ways of ensuring national security (Ways) are: *"the defense dimension; the public order dimension; the informational dimension, counter-information, and security dimension; the economic and energy dimension; the diplomatic dimension; the crisis management dimension; the educational, health, social and demographic dimension"*[36].

These are the main benchmarks for defining possible directions of action and identifying risks and threats to national security.

[34] *Ibid*, p. 10.
[35] *Ibid*, pp. 18-22.
[36] *Ibid*, pp. 18-22.

In conclusion, the *Ends, Ways & Means* model applies well to the National Defense Strategy, with the mention that *Means* can be detailed, that is, the concrete way of developing those presented directions should be identified, thus offering the premises of their materialization. Following the analysis, I identified the national goals (*Ends*), I identified *Ways*, but I did not identify *Means* well represented. If means are not defined, this aspect is also transmitted to strategic documents that extract their directions from this national reference document.

Having validated the method of realising a strategy, I consider that these aspects are a result of the theory and art of the Romanian school that uses the theory and applies the art of modern strategic thinking.

THE PLACE OF A MARITIME STRATEGY

Next, I would like to identify the place of a maritime strategy, which extracts its purpose and objectives from the directions specified in the national strategy. Also from here, it extracts his foundation and a military strategy. Having developed a national defense strategy, there is the premise of developing a military strategy that meets the country's security guidelines.

A maritime strategy of the Black Sea must also represent a national priority institutional approach. The advantages of a maritime strategy are reflected by the existence of security, of the favorable environment for the development of the economy, which leads to the multiplication of the country's welfare. From this point of view, maritime security is very important.

The maritime component of security is another national objective that should not be neglected, specified in the framework of the national strategy in *Chapter I*[37]. Thus, a maritime strategy of the Black Sea must also represent a national priority institutional approach. The advantages of a maritime strategy are reflected by the existence of security, of the favorable environment for the development of the economy, which leads to the multiplication of the country's welfare. From this point of view, maritime security is very important.

A maritime strategy must occupy a wider space, well defined, in the national strategy, in the military strategy as well as in the military-strategic plans. In my opinion, there are all the premises

[37] *Ibid*, p. 10.

for developing a maritime strategy that clearly defines national interests in the maritime environment. I recall that the strategy represents a means of achieving the goals defined by the policy, thus, the maritime strategy represents the means by which the national interests in the maritime environment are fulfilled.

It is precisely this aspect of my approach that I consider being the novelty of this article, which consists in identifying the place of the maritime strategy within the National Defense Strategy and the Military Strategy.

The manifestation of national interests in the maritime environment has a direct connection with the maritime power of the state. The components of maritime power must be subjects of analysis of a maritime strategy. The most visible component of maritime power is the naval power, represented by the Romanian Navy.

The manifestation of national interests in the maritime environment has a direct connection with the maritime power of the state. The components of maritime power must be subjects of analysis of a maritime strategy. The most visible component of maritime power is the naval power, represented by the Romanian Navy. The capabilities of this component (means) are the most important vector for achieving the objectives of the maritime strategy. I believe that together with the naval forces, human resources and education are the most accessible means of achieving these objectives, components that must be fully exploited and exploited.

In my opinion, after analysing the content of the previous strategies, I consider that they did not represent the maritime strategies well. I also bring in your attention to the fluvial component. Let us not forget the Danube River! In this direction, I consider that a maritime strategy must also include Romanian fluvial interests. I do not think we can yet speak of the opportunity to develop a strategy for the Danube River, because the Danube River is not fully exploited, but we can approach the field within the Romanian maritime strategy.

Therefore, I consider two variants of presenting Romania's maritime interests. In the first version, I consider its own maritime strategy. In the second variant, I believe that this can be found in the national defense strategy. The provocative question is how to represent a maritime strategy in the national defense strategy and in the military one. But I will resume this topic in another dedicated work.

In the hypothesis that we are not yet prepared to have a separate maritime strategy, in this variant, I propose a separate chapter in the national defense strategy, which defines maritime and fluvial security.

A brief comparative analysis

In order to make a comparative picture, I will analyse how the issue of national and maritime security is approached in the neighboring countries and I have chosen two partners and allies, Bulgaria and Poland, identifying the strategic model and directions of the main strategic documents.

I chose Bulgaria, because we have a lot of commonalities regarding the manifestation of regional interests, to see what their vision is about security and how they develop their capabilities to ensure it. I also chose Poland because I observed a considerable involvement in the strengthening of regional security, an increase in the capabilities of action and a political consensus that supports the measures provided for in the national security strategy.

Following the analysis of the Bulgarian national strategy, I found that it is also built on the Anglo-Saxon model, adopted after joining NATO, and defines in great detail the objectives, ways, and means necessary to strengthen national security, the army is the main vector to guarantee the fulfillment of political intentions, the necessary means being of human, material, informational and financial nature.

Following the analysis of the Bulgarian national strategy, I found that it is also built on the Anglo-Saxon model, adopted after joining NATO, and defines in great detail the objectives, ways, and means necessary to strengthen national security, the army is the main vector to guarantee the fulfillment of political intentions, the necessary means being of human, material, informational and financial nature[38]. It should be noted that our neighbors have their own maritime strategy, through which they promote their own maritime interests but also those of the community, promoting measures to cooperate with their neighbours[39].

Analyzing the Poland Security Strategy[40], I found that it is very dynamic and adaptive to the international Security environment.

[38] *National Defense Strategy, Sofia, 2011*, conform www.strategy.bg, retrieved on 27.02.2020.
[39] https://www.moew.government.bg/en/water/marine-environment/marine-strategy-of-republic-of-bulgaria/ retrieved on 27.02.2020.
[40] *National Security Strategy of the Republic of Poland*, Varsaw, 2014

The Poland defense strategy starts from the objectives set at the political level, sets the ends, to increase the deterrent capacity, establishes the ways, i.e. modeling the desired form of the Polish army, thus being called the means by which these objectives are achieved.

I noticed that in 2016, Poland launched a new strategic concept, very realistic, that would respond to security needs under the conditions of A2AD threats[41], defining very clearly the objectives, the ways and means by which to achieve them. The document, however, emphasises and details the ways in which the strategic objectives can be achieved with a deadline established in 2032, the focus being the defense capabilities, the command, and control system, the responsiveness. The political environment plays an important role[42]. Interestingly, the effects of applying this strategy are already being observed, with the Polish Armed Forces being highly visible at regional, alliance and EU levels, which gives it a credible security generator position.

In 2016, Poland launched a new strategic concept, very realistic, that would respond to security needs under the conditions of A2AD threats, defining very clearly the objectives, the ways and means by which to achieve them.

Concerning the Poland maritime strategy[43], I identified that the strategic document contains the assessment of the maritime security environment, the threats, risks, opportunities and challenges, the assessment of the country's maritime forces, defines the national interests and the strategic objectives. The elements of tradition, historical and social-cultural context are presented. It basically represents a coherent dialogue forum that requires a synergistic and integrated approach[44]. In my opinion, it is a very well-balanced strategic document, the *Ends, Ways & Means* model being well applied[45].

Following the analysis, I noticed two different security approaches, one declarative and one actionable. The Polish example is

[41] https://www.defence24.com/polish-national-defence-concept-new-division-and-5th-generation-fighter-aircraft, retrieved on 29.02.2020.
[42] https://www.gov.pl/web/national-defence/polish-defence-in-the-perspective-of-2032, retrieved on 29.02.2020.
[43] https://en.bbn.gov.pl/ftp/dok/SKBMRPENG.pdf retrieved on 27.02.2020.
[44] *Ibid*, p. 6.
[45] Tomasz Szatkowski, Undersecretary of State at the Polish Ministry of Defence, https://www.defence24.com/polish-national-defence-concept-new-division-and-5th-generation-fighter-aircraft, retrieved on 29.02.2020.

a benchmark for the member countries on the eastern flank of the Euro-Atlantic bloc, which must be followed. They identified the potential and opportunities that generated the awareness of the proactive adaptation to the security environment threats and identified the ways of expressing the national intentions. It is worth noting that Poland has indeed found the key to success, which I identified at the level of political will.

CONCLUSIONS

Following the presentation of a possible solution for the realization of a strategy and the analysis of the content of the national defense strategy, I consider that a strategy must be defined by the following characteristics: be proactive and anticipatory; to be hierarchical, that is to define clearly the objectives, to define and identify the ways of accomplishment, to identify and to offer the possibility of developing the means for the accomplishment of the objectives. Basically, it has to strike an appropriate balance between ends, ways, and means. Political objectives must prevail in one strategy.

I believe that the national defense strategy is well structured, but even though I have clearly identified the ends and the ways, I have not found well represented the concrete means of achieving the political objectives.

As a specialist in the field of maritime operative art, I felt the need to promote such an approach, because an articulated strategy of the Black Sea does not exist and its realization is an effort that requires time and resources.

Successfuly promoting the maritime strategy depends on the awareness of the political class of the importance of the manifestation of the maritime power, of the valorisation of the resources of the maritime and fluvial environment.

Successfuly promoting the maritime strategy depends on the awareness of the political class of the importance of the manifestation of the maritime power, of the valorisation of the resources of the maritime and fluvial environment. I believe that the fulfillment of national maritime interests is achieved by creating and developing a maritime power supported by the existence of a naval strategy that emphasizes the defense of the interests of the state at sea and river.

I believe that the novelty of this article consists in the attempt to identify the place of the maritime strategy in the framework of the National Defense Strategy and the Military Strategy, which is the level of representativeness and which is the opportunity of such an approach, in relation to Romania's maritime power.

The missing link in the national defense strategy is defined by the national maritime and fluvial policy. I think that for the moment, Romania is not prepared to have a maritime strategy on its own, but in the long term, this objective must be achieved. That is why, in my opinion, I think it is appropriate to start such a process, for which I personally started the promotion. Such an approach, the promotion of Romania's maritime strategy is the result of an integrated vision regarding the motivation of protecting the maritime and fluvial interests of our country.

BIBLIOGRAPHY

1. ***, *National Defense Strategy, Sofia, 2011*, www.strategy.bg.
2. ***, *National Security Strategy of the Republic of Poland*, Varsaw, 2014.
3. ***, *Ordonanța nr. 52, (art. 4) din 12 august 1998 privind planificarea apărării naţionale a României*, republished.
4. ***, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019. O Românie puternică în Europa și în lume/The National Defence Strategy 2015-2019 – A Strong Romania within Europe and the World*, The Presidential Administration, București, 2015.
5. Antoine Henri Jomini, *Principes de la stratégie*, Paris, 1818; translated from German to French.
6. David M. Glantz, Harold S. Orenstein, *The Evolution of Soviet Operational Art, 1927-1991: The Documentary Basis,* vol I., Franc Cass London, 1995.
7. Colin Gray, John Baylis, James Wirtz, *Strategy in the Contemporary World*, Oxford University Press, 2019.
8. Gregory D. Miller, Chris Rogers, Francis J.H. Park, William F. Owen, Jeffrey W.Meiser, *On Strategy as Ends, Ways, and Means*, Journal of the US Army War College 47(1):125-126, January 2017.
9. Mircea Mureşan, Costică Ţenu, Lucian Stăncilă, *Corelaţia artei militare cu fenomenul militar contemporan, Curs de artă militară*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2005.
10. Gheorghe Văduva, *Principii ale războiului şi luptei armate-realităţi şi tendinţe*, Universitatea Naţională de Apărare, Centrul de Studii Strategice de Apărare şi Securitate, Bucureşti, 2003.
11. Wilhelm Rustow, *The War for the Rhine Frontier 1870, its Political and Military History*, Vol. 2, p. 281.

WEBOGRAPHY:

1. dexonline.ro
2. https://www8.gsb.columbia.edu/articles/ideas-work/von-clausewitz-war-six-lessons-modern-strategist
3. https://devcentral.f5.com/s/articles/he-who-defends-everything-defends-nothinghellip-right
4. https://www.globalsecurity.org/military/library/policy/usmc/mcdp/1-1/mcdp1-1_chap2.pdf
5. https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019
6. https://www.moew.government.bg/en/water/marine-environment/marine-strategy-of-republic-of-bulgaria/
7. https://www.defence24.com/polish-national-defence-concept-new-division-and-5th-generation-fighter-aircraft
8. https://www.gov.pl/web/national-defence/polish-defence-in-the-perspective-of-2032
9. https://en.bbn.gov.pl/ftp/dok/SKBMRPENG.pdf.

ROMANIAN MILITARY THINKING

OPERATION DESIGN AT TACTICAL LEVEL

Lieutenant Cătălin CHIRIAC
"Carol I" National Defence University, Bucharest

The release of the Operations Planning Manual at national level has led to rethinking of how to carry out the operations planning, at all levels of the military art: strategic, operational and tactical.

By implication, the new concepts and approaches proposed through the manual were taken up, explained and adapted to a certain extent to national specificities and applied by all levels, even though some of them needed different clarifications and approaches (such as operation design).

Keywords: operation, tactical level, operation design, planning documents, operational framework.

INTRODUCTION

The purpose of this article is to open up that dialogue that can lead to clarifying the meaning of the concept of *operations design* and how it can be developed at operational and especially tactical levels. At the national level, there is a well-detailed planning process for the operational level which is based on the main concepts and tools of the operations design, but unfortunately there are no doctrinal references to the necessity and development of this concept for the tactical level.

Appeared in the military planners language with the now well-known COPD[1], *the operations design* was intended to be the process to base the "*development of campaign/operational concept and planning documents*"[2]. The use and development of this concept has generated many problems for military planners at the operational level, and, above all, from the tactical level, through its lack of explanation in the manuals or in specific operational planning doctrines and the lack of examples. Although *the Operations Planning Manual* ensures that the concept is defined and places it in the process carried out by the operational level, it does not provide any clarifications or details on the approach of this concept by the tactical level. In these circumstances, I believe that the main elements that require deepening and a close clarification relate to the level and the way in which the operations design can be developed.

The operations design was intended to be the process to base the "development of campaign/ operational concept and planning documents".

One of the most difficult issues to which planning groups or staffs from tactical level must find an answer is *the existence and development of the operations design* at this level. The problem is difficult because this concept is detailed only for the strategic and operational level and there is some uncertainty when discussed at the tactical level.

[1] *Allied Command Operations Comprehensive Operations Planning Directive. At national level, the provisions of the COPD are contained in the Operations Planning Manual/Manualul de planificare a operațiilor*, Statul Major General, București, 2016.
[2] *** *Doctrina Armatei României*, Statul Major General, Bucureşti, 2012, p. 150.

Although *the Operations Planning Manual* makes it clear that *"at national level, the design takes two dimensions – strategic design and design at operational level"*[3], it does not provide further clarification on the approach to the tactical level, while the same manual represents the foundation for the development of specific planning manuals of different force categories (services).

Even though the appearance of the concept has questioned at some point the existence and conduct of the planning process, the design should not be seen as a replacement for it. The current planning processes for strategic and operational levels clearly determine when the design is deployed, the specific products of this process and the way they ensure the fluidity of the subsequent process. In 2009, the former commander of US Joint Forces Command, US General James Mattis, established the elements of the relationship between design and planning: "*Design does not replace planning, but planning is incomplete without design. The balance between the two varies from operation to operation as well as within each operation. […] Executed correctly, the two processes always are complementary, overlapping, synergistic, and continuous"*[4]. In these circumstances, the design and planning make it possible to transform the broad direction and orders of the commanders of the strategic and operational echelons into concrete missions and tasks for the tactical level.

In 2009, the former commander of US Joint Forces Command, US General James Mattis, established the elements of the relationship between design and planning: "Design does not replace planning, but planning is incomplete without design. The balance between the two varies from operation to operation as well as within each operation. […] Executed correctly, the two processes always are complementary, overlapping, synergistic, and continuous".

OPERATIONAL DESIGN AT OPERATIONAL LEVEL

At operational level, the operation design is both a process and a product. It is a process due to the concrete steps to be taken to carry it out and a product because the application of the process aims at a combination of specific information and elements needed to continue the process. Produced as a result of the application of the operative arts[5],

[3] *** *Manualul de planificare a operaţiilor*, *op. cit.*, p. 18

[4] *General James Mattis*, Former Commander, US Joint Forces Command, *Vision for a Joint Approach to Operational Design*, 6 October 2009, available at www.smallwarsjournal.com/blog/usjfcom-releases-approach-to-operational-design-vision, retrieved on 23.01.2020.

[5] *Manualul de planificare a operațiilor defines operational art as the employment of the military instrument to attain strategic and/or operational objectives through the design, organisation, integration and conduct of campaigns, operations and battles, linking military strategy and tactics.*

the operation design is the expression of the Commander's vision regarding the transformation of the unacceptable situation from the start of the campaign, into a number of acceptable conditions at the end of it[6].

Achieving the design through the united input of the planning group and the commander allows the operational level to view the overall picture of the whole campaign and identify the elements that ensure smooth tactical actions. While the planning group is responsible for the development of the *operational framework* (series of specific concepts identified or determined in accordance with current specifications), the structure commander is required to establish and issue the *initial intention*. Together, these two elements form **the initial operational design**[7].

At national level[8], the operational framework is developed based on operational design specific concepts, which are aligned to those identified at Alliance level. Used in a progressive sequence, design concepts are needed to understand operational requirements and ease planners activities. National documents comprise 12 concepts, such as: desired end state, transition and termination, objectives, effects, performance and effectiveness indicators, criteria for measuring success, centres of gravity and the associated capabilities, requirements and vulnerabilities, decisive points and conditions, lines of operations, the geometry of the operation, sequence of actions and phases of the operation (established by applying the following operational concepts: timing, synergy and multiplier effect, simultaneity and depth, maneuver, operational tempo and main effort), contingencies – branches and sequels, culmination, operational breaks, direct and indirect approach[9].

ROMANIAN MILITARY THINKING

Achieving the design through the united input of the planning group and the commander allows the operational level to view the overall picture of the whole campaign and identify the elements that ensure smooth tactical actions. While the planning group is responsible for the development of the operational framework (series of specific concepts identified or determined in accordance with current specifications), the structure commander is required to establish and issue the initial intention. Together, these two elements form the initial operational design.

[6] *** COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, 4 October 2013, p. 4-52.

[7] ***, *Manualul de planificare a operaţiilor*, Statul Major General, Bucureşti, 2016, p. 114.

[8] ***, *Doctrina planificării operaţiilor în Armata României*, Statul Major General, Bucureşti, 2013, p. 40.

[9] Concepts are detailed in *Doctrina planificării operaţiilor în Armata României*, *op. cit.*, pp. 40-57.

But at operational level, the operational framework is achieved during Phase 3 of the planning process (*operational estimate*), by establishing *the decisive conditions, effects, operational and non-military actions, lines of operations, sequences and phases of the operation, branches and sequels of the lines of operation*[10]. This approach should be seen as a *logical route to the preparation of the operational framework, but may vary depending on the commander's directions and the planning group's experience*[11].

The commander's intention is stated during the *Mission analysis briefing*, at which point the operational framework is also validated, while the operational design as a whole will be approved during *the Decision briefing.*

According to the provisions of the Romanian Army Doctrine, the tactical level represents the level "at which clashes and battles are planned and executed to accomplish the military objectives of the units and large tactical units".

OPERATION DESIGN AT TACTICAL LEVEL

According to the provisions of the Romanian Army Doctrine, the tactical level represents the level *"at which clashes and battles are planned and executed to accomplish the military objectives of the units and large tactical units"*[12]. The documents drawn up in support of planning and evaluation of operations or targeting process shall further specify the meaning that the tactical level begins with the force categories and operational components. This reality, irrespective of the force category (land, air, naval or special operations), requires that the operations planning for this level must meet the requirements and specificities of all component structures and the specificities of military specialty. Taking these elements into account, performing the operational design at the tactical level raises several questions about its opportunity and how it can be done, as well as the level up to which it can be applied.

I believe that the main issue of the operation design at national level is, first and foremost, its own definition. At NATO level, there is in the military literature the notion of "*operational design*" which, at national level, has been translated and implemented under the name

[10] ***, *Manualul de planificare a operaţiilor*, *op. cit.*, pp. 116-117.
[11] *Ibid,* 116.
[12] ***, *Doctrina Armatei României*, *op. cit.*, p. 159.

"*operation design/designul operației*" and not as "*operational design/designul operațional*", as would have been more accurate. For correct information, within the Alliance there are "*operational design*" and "*operations planning*" to distinguish between the level of planning and operation[13].

Taking and translating the word "*operational*" from English with the word "*operațional*", but at the same time also with the word "*operativ*", has led to many difficulties or anomalies in national textbooks or doctrines. In these circumstances, the level between strategic and tactical is the *operative level* that makes an assessment of the *operational environment*, develops both "*operational*" and "*operative*" plans and meets *operational requirements*. *The operational design* at this level is based on "*operational framework"* (correctly taken from the English „*operational framework*") and not on "*operative framework"* (in the logic of taking over the term "operational") and the intention of the commander.

Within the Alliance there are "operational design" and "operations planning" to distinguish between the level of planning and operation.

While at NATO level, "*operational design*" is linked to its operational level and its specific operation, at national level "*operation design*" can be understood as addressing to all structures carrying out operations. This has also introduced this uncertainty in the use of the concept.

Another aspect that makes it difficult to develop the operational design at the tactical level is the characteristics of the level itself. Tactical level analysis requires consideration of a quite large number of structures, starting from the force categories and operational components and ending with battalion or even company-level subunits. In these circumstances, it is impossible to perform the operation design, as it is impossible to comply with the standard format of the concept for all these structures. However, under these conditions the tactical level option would be limited to determining which structures can meet the requirements of the operation design.

One final aspect to be taken into account when discussing the operation design at tactical level is its concepts, which are simply

[13] COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, 4 October 2013, p. 1-3.

not characteristic of this level, regardless of the efforts of planners in this manner. I believe that the main concepts that cannot be identified at tactical level, in the sense that they can contribute to the operation design, are *decisive conditions*, *effects* and *lines of operations*.

The primary element from which to start when discussing the operation design is the provisions of the planning documents. In order to be able to carry out the operation design, there shall be an *operational framework* and a *commander's intention*. *Even if there is a commander's intention but, an incomplete operational framework, lacking in any important elements, the operational design, as outlined above, cannot be discussed.* At both national and Alliance level, it is quite clear that, at the joint level, the operational framework and, consequently, the design is developed by establishing *decisive conditions along lines of operations leading to the achievement of operational level objectives and thus contributing to the achievement of the strategic objectives and the final end state*[14]. I believe that the use of the term *"operation design"* must be made in accordance with the definition, the terms and, above all, their meaning defined by the specific documents.

The primary element from which to start when discussing the operation design is the provisions of the planning documents. In order to be able to carry out the operation design, there shall be an operational framework and a commander's intention. Even if there is a commander's intention but, an incomplete operational framework, lacking in any important elements, the operational design, as outlined above, cannot be discussed.

In these circumstances, analysis of the definitions and characteristics of the main concepts referred to above, as set out in the specific national documents, leads to the following main elements:

❖ *Decisive conditions* are critical to achieving an operational objective, the scope of this concept being far more comprehensive than the *decisive points*. While the decisive points can be used to achieve the operational design of force-on-force operations[15], the use of decisive conditions is much closer to the reality of the operating environment and specific to "*current operations, as it better reflects the military contribution to the comprehensive approach*"[16]. The same conclusion can be drawn from the analysis of the definition of concepts in *Table 1*. For the tactical level, it is therefore appropriate to use,

[14] ***, *Manualul de planificare a operaţiilor*, *op. cit.*, p. 20 and COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, 4 October 2013, p. 1-13.
[15] ***, COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, 4 October 2013, p. 4-52.
[16] ***, *Doctrina planificării operaţiilor în Armata României*, *op. cit.*, p. 49.

where the situation requires, the "*decisive points*" and not the decisive conditions, which are far too generous and complex for this level. But under these circumstances, no further concordance with the definition and concepts of the above operational framework is achieved.

Decisive point	Decisive condition
A point from which a hostile or friendly centre of gravity can be threatened. This point may exist in time, space or in the information environment.	A combination of circumstances, effects, or a specific key event, critical factor, or function that, when achieved, allows commanders to gain a marked advantage over an opponent or contribute materially to achieving an operational objective

Table 1: Definition of the terms decisive point and decisive condition[17],[18]

❖ In general, an effect can be defined as "*a change in the physical or behavioural state of a system or system element, which is created by the result of one or more actions*"[19]. Characteristic of this concept is that the effects are used in planning and carrying out operations at strategic and operational levels only[20], with tactical levels focusing on "*the tasks required to fulfil missions which, ultimately, lead to the achievement of the desired impacts at strategic and operational level*"[21]. Even if tactical level actions are logically followed by the normal effects of their development (according to the effect definition), I believe that *the effects* cannot be quantified at the true value at this level or, under certain conditions, may be confused with the objectives set at both the upper echelon level, and within its own structure. It is therefore logical that the tactical level should strive to identify the tasks needed *to carry out the received missions* from the operational level and not to *identify*

In general, an effect can be defined as "a change in the physical or behavioural state of a system or system element, which is created by the result of one or more actions".

[17] *Doctrina Armatei României*, *op. cit.*, pp. 148, 167.
[18] ***, *NATO Glossary of Terms and Definitions (English and French)*, North Atlantic Treaty Organization, NSO, 2016, p. 40.
[19] ***, *Manualul de planificare a operaţiilor*, *op. cit.*, p. 187.
[20] *Ibid*, p. 17 and COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, 4 October 2013, p. 1-11.
[21] *** *Manualul de planificare a operaţiilor*, *op. cit.*, p. 81.

their effects. However, at tactical level, the structure commanders may make recommendations on actions that may be carried out by their own forces to achieve the effects set at the operational level;

❖ The line of operations is "*a logical sequence linking in time and space the effects and decisive points, on the road to the centre of gravity, in order to achieve an operational objective, in a campaign or operation*"[22] and, usually, there is a line of operations for each objective[23]. If the line of operations links effects, decisive points and objectives, logically, the absence of one or more constituent elements entails its cancellation. We therefore consider that, in the absence of decisive effects or conditions, no tactical lines of operations can be identified.

The concepts of operation design are logically developed – as previously mentioned – and are in a determining relationship, in the way that identifying a concept leads to the establishment and identification of the next. At the same time, however, the absence of a concept can create problems in identifying another concept or even make it impossible to establish the operational framework as it has been defined.

CONCLUSION

The concepts of operation design are logically developed – as previously mentioned – and are in a determining relationship, in the way that identifying a concept leads to the establishment and identification of the next. At the same time, however, the absence of a concept can create problems in identifying another concept or even make it impossible to establish the operational framework as it has been defined, in which situation is the tactical level today.

The operation design as adopted in documents elaborated at national level cannot be developed at tactical level due to the arguments presented above. However, there is a possibility that this may happens, either because of the provisions of the manuals at this level or because of an overzealous approach of the commanders or the planning group, by force-action of the effects, decisive conditions or lines of operations. *The effects* of such an approach lead to an overload of the staff involved and unjustified congestion of the process, with time being increasingly limited.

[22] *Ibid*, p. 190.
[23] *Ibid*, p. 117.

BIBLIOGRAPHY

1. ***, *Allied Command Operations Comprehensive Operations Planning Directive – COPD Interim V2.0*, SHAPE, 2013.
2. ***, *Doctrina Armatei României*, Statul Major General, Bucureşti, 2012.
3. ***, *Doctrina planificării operaţiilor în Armata României*, Statul Major General, Bucureşti, 2013.
4. ***, *Manualul de planificare a operaţiilor*, Statul Major General, Bucureşti, 2016.
5. General James Mattis, Former Commander, US Joint Forces Command, *Vision for a Joint Approach to Operational Design.*

ROMANIAN MILITARY THINKING

CYBERWAR AND CYBERTERRORISM. FEATURES AND ANSWERS TO THESE THREATS

Colonel (r.) Romică CERNAT, PhD

In recent years, cyberspace has taken increased strategic importance as states have begun to think of it as a domain similar to land, sea, and air, that must be secured to protect their national interests. Cyberattacks are now a common element of international conflict, both on their own and in the broader context of military operations. Attacks in cyberspace have been amplified and diversified in terms of actors and methods. Because states have become more dependent on information technology and critical network infrastructure components, many questions arise about whether a state is organised properly to defend its digital strategic assets. Cyberspace integrates the operation of critical infrastructures, as well as governmental and national security institutions and commerce. Because cyberspace transcends geographic boundaries, much of it is outside of control and influence of a state.

Keywords: cyberwar, cyberterrorism, cybercrime, computer virus, computer network, information system.

PRELIMINARY CONSIDERATIONS

The concept of *"Cyber-attack"* is a relatively recent term and refers to a wide range of activities conducted through the use of information and communication technology (ICT). The use of Distributed Denial of Service (DDoS) attacks has become a widespread method of achieving political objectives through the disruption of online services. In this type of attacks, a server is overwhelmed with Internet traffic so that access to certain websites is degraded or denied. *Stuxnet* virus appearance, in June 2010, which some consider the first cyber-attack, revealed that cyber-attacks could have a destructive and lasting effect. Created to sabotage Iran's nuclear programme, Stuxnet, the destructive system of computer software, attacked the industrial computerised control systems on which nuclear centrifuges that produce enriched uranium operate, having as finality the physical self-destruction of the facilities. Recent international events have raised questions about the situation when a cyberattack could be considered an act of war and what kind of response options are available to the victim states.

Stuxnet virus appearance, in June 2010, which some consider the first cyber-attack, revealed that cyber-attacks could have a destructive and lasting effect. Created to sabotage Iran's nuclear programme, Stuxnet, the destructive system of computer software, attacked the industrial computerised control systems on which nuclear centrifuges that produce enriched uranium operate, having as finality the physical self-destruction of the facilities.

Given those presented above, it is necessary that each state should take the necessary measures and develop the mechanisms at the national level and participate, at the European and international level, in the field of networks and information security systems to ensure a common high level of security and boost cooperation in the domain[1].

The cyber-attacks on *Sony Entertainment* illustrate the difficulties in classifying attacks and formulating a policy response. On 24 November 2014, Sony Corporation has been the subject of a cyber-attack which disabled its ICT systems, destroyed data and workstations and accessed internal e-mails and other data. The Federal Bureau of Investigation (FBI) and the Director of National Intelligence (DNI) of the United States of America attributed the cyber-attacks to the North Korean government. North Korea denied involvement in the attack, but praised a hacktivist group called the *"Guardians of Peace"*

[1] *Law no. 362/2018 on ensuring a common level of security of networks and information systems*, in the *Official Gazette,* Part I no. 21 of 9 January 2019, p.1.

for having done a *"righteous deed"*. During a press conference on 19 December 2014, President Obama pledged to *"respond proportionally"* to North Korea's alleged cyber aggression *"in a place, time and manner of our choosing"*[2]. President Obama categorised the incident as an act of *"cyber-vandalism"*, while other analysts labelled it as an act of cyberwar.

This incident illustrates the difficulties in classifying cyber-attacks, with respect to the actors involved and their motivations, as well as issues of sovereignty regarding the site where the actors were physically located. With the globalised nature of the Internet, authors can launch cyber-attacks from anywhere in the world and direct the attacks through servers belonging to third-party countries. A deep analysis of major cyber-attacks on government agencies, companies in the defence sector and high-tech, or economic crime with losses of more than one million dollars highlights the extent of this phenomenon[3]. Was the cyber-attack on Sony, a private corporation with headquarters in Japan, an attack on the USA? Further, could it be considered an act of terrorism, use of force or a cybercrime? In categorising the attack on Sony as an act of *"cyber vandalism"*, which usually includes compromising websites and is generally the realm of politically motivated actors known as the *"hacktivists"*, President Obama had reservations about what kind of response could be considered *"proportional"* and against whom. Another potential question could be related to the circumstances under which the USA would commit troops to respond to a cyber-attack. In a logical relationship is also the question of whether the USA and other powerful states have an effective deterrent strategy in place. The US acting DNI, Clapper, said about cyberwar actors that *"if they get global recognition, at low cost and will no consequence, they will do it again and keep doing it again until we push back"*[4].

With the globalised nature of the Internet, authors can launch cyber-attacks from anywhere in the world and direct the attacks through servers belonging to third-party countries. A deep analysis of major cyber-attacks on government agencies, companies in the defence sector and high-tech, or economic crime with losses of more than one million dollars highlights the extent of this phenomenon.

[2] Barack Obama, *"Remarks by the President in Year-End Press Conference"*, 12 December 2014, in *The White House Office of the Press Secretary*, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference, retrieved on 20.12.2019.

[3] *"Significant Cyber Incidents Since 2006"*, in *Center for Strategic & International Studies*, https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa, retrieved on 07.01.2020.

[4] Chris Strohm, *"FBI Provides More Proof of North Korea Link to Sony Hack"*, 7 January 2015, in *Bloomberg*, https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony, retrieved on 20.12.2019.

THE STATES AND INTERNATIONAL BODIES STANCE TO CYBERWARFARE

Critical infrastructure has long been subject to physical threats and is now increasingly exposed to the risk of attacks in cyberspace[5]. Cyberwar is typically conceptualised as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional use of force. Criminals, terrorists and spies, in their work, rely heavily on cyber-based technologies to accomplish the organisational objectives. Cyber terrorists are individuals sponsored by state and non-state actors that engage in cyber-attacks to achieve their objectives. Transnational terrorist organisations, insurgents and jihadists have used the Internet as a tool for planning attacks, radicalisation and recruitment as a method of propaganda dissemination, and as a means of communication, as well as for disruptive purposes.

There are no clear criteria, yet, for determining whether a cyber-attack is a crime, an act of hacktivism, terrorism or the use of force by a state equivalent to an armed attack. Similarly, no international, legally binding instruments have been yet drafted, which explicitly regulate inter-state relations in cyberspace.

In September 2012, the US Department of State took a public stand on the fact that cyber-attacks could be interpreted as a use of force in accordance with Article 2, paragraph 4, of the UN Charter and customary International Law. According to the Legal Advisor of the Department of State at that time, Harold Koh, *"cyber activities that proximately result in death, injury or significant destruction would likely be viewed as a use of force"*[6]. The examples given in Koh's remarks included triggering the destruction of a nuclear power plant, opening a dam and causing flood damage or causing airplanes to crash by interfering with air traffic control. Focusing more on the effects produced rather than the means with which they are carried out, this definition of cyberwar integrates easily within the existing international legal framework. If an actor employs a cyber-mean to produce kinetic effects that could

Cyber terrorists are individuals sponsored by state and non-state actors that engage in cyber-attacks to achieve their objectives. Transnational terrorist organisations, insurgents and jihadists have used the Internet as a tool for planning attacks, radicalisation and recruitment as a method of propaganda dissemination, and as a means of communication, as well as for disruptive purposes.

[5] The White House, in *National Strategy for Counterterrorism of the United States of America*, October 2018, p. 19, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf, retrieved on 20.12.2019.

[6] Harold Hongju Koh, *"International Law in Cyberspace"*, in *US Department of State*, *Archived content*, 18 September 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm, retrieved on 20.12.2019.

justify the use of military force in other circumstances, then the use of that weapon can be treated as use of force.

Koh explained that cyber-attacks on information networks during an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyber-attack with a proportional use of military force. In addition, *"computer network activities that amount to an armed attack or imminent threat"* may trigger a state's right to self-defence in accordance with Article 51 of the UN Charter provisions. Koh cites in his remarks the 2011 International Strategy for Cyberspace (ISC), which provides that *"when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country"*[7]. One of the defence objectives of ISC is to work internationally *"to encourage responsible behaviour and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend national assets"*[8]. A growing awareness of the environmental threats in cyberspace has led to two major international processes aimed at developing international expert consensus among international cyber authorities.

The Tallinn Manual, as it is known, was published in 2013. It sets out 95 "written severe rules" governing the consequences of cyber conflict in relation with the sovereignty and responsibility of the state, the law of armed conflict, humanitarian law and the law of neutrality. The Tallinn Manual is an academic text and although it offers reasonable justifications for the implementation of international law, it is not binding, and the authors stress that they do not speak for NATO or the CCDCE.

NATO regulations for cyberspace. A year after the 2007 DDoS attack on Estonia, NATO established the Cooperative Cyber Defence Centre of Excellence (CCDCE) in Tallinn, Estonia. CCDCE hosts workshops and courses of law and ethics in cyberspace, as well as cyber defence exercises. In 2009, the Centre convened an international group of independent experts to develop a manual to be approved by a law and regulate how to act in case of a cyber-war. The Tallinn Manual, as it is known, was published in 2013[9]. It sets out 95 *"written severe rules"* governing the consequences of cyber conflict in relation with the sovereignty and responsibility of the state, the law of armed conflict, humanitarian law and the law of neutrality. The Tallinn Manual is an academic text and although it offers reasonable justifications

[7] *"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"*, May 2011, in *US Department of State*, p. 14, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ international_strategy_for_cyberspace.pdf, retrieved on 20.12.2019.

[8] *Ibidem*. p.12.

[9] *"Tallinn Manual on the International Law Applicable to Cyber Warfare"*, in *The NATO Cooperative Cyber Defence Centre of Excellence*, p. 5, http://csef.ru/media/articles/3990/3990.pdf, retrieved on 06.01.2020.

for the implementation of international law, it is not binding, and the authors stress that they do not speak for NATO or the CCDCE.

Arguably, NATO currently does not have a clear position on the application of Articles 4 and 5 of the NATO Treaty in cyberspace and presently does not define a cyber-attack as a clear military action. The Tallinn Manual equates a use of force to those cyber operations whose *"effects… are analogous to those that would result from an action otherwise qualifying as a kinetic armed attack"*[10]. If an attack is deemed to be orchestrated by a cyber-criminal organisation, whether politically or financially motivated, then it may be the attacked state responsibility to select an appropriate response within its jurisdiction. However, the transnational nature of most criminal organisations in cyberspace can complicate decisions on jurisdiction.

Law of armed conflict on cyberwar. Reprisals in response to armed attacks are permitted in international law, when a belligerent state violates international law during peacetime, or the law of armed conflict, during wartime. However, the term *"armed attack"* has no legal definition and is still open to interpretation, completion and change, with respect to cyber-attacks. The so-called *"Law of War"*, also known as the law of armed conflict, embodied in the Geneva and Hague Conventions and the UN Charter, may under certain circumstances apply to cyber-attacks, but no attempts recorded by the states to implement it, or the existence of specific agreements regarding the applicability, its relevance under these conditions remains unclear. The application becomes complicated, and also, because of the difficulties in attribution, the potential use of remote computers, as well as the possible harm to third parties resulting from cyber counterattacks, which could be difficult to be controlled or contain. In addition, territorial boundaries issues and what constitutes an armed attack in cyberspace remain. The law's enforcement would seem clearest in situations where a cyber-attack causes physical damage, such as disruption of electric grid. As mentioned above, the *Tallinn Manual* addresses many of these questions[11]. In the absence of a legal definition of what constitutes an *"armed attack"* in cyberspace,

ROMANIAN MILITARY THINKING

In the absence of a legal definition of what constitutes an "armed attack" in cyberspace, Professor Michael Schmitt suggests the following criteria for analysis in accordance with international law: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.

[10] *Ibidem,* p.54.

[11] Oona A. Hathaway, *"The Law of Cyber-Attack",* in *California Law Review, Vol. 100, No. 4, 2012,* pp.6-23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932, retrieved on 06.01.2020.

A series of UN General Assembly resolutions relating to cybersecurity have been adopted over the past 19 years. One resolution requested for the convening of a report from an international group of government experts from 15 states, including the USA. The stated goal of this process was to build a "cooperation for a peaceful, secure, resilient and open ICT environment" by reaching an agreement on the "norms, rules and principles of responsible behaviour by States" and identifying capacity-building measures for confidence and capabilities, including for exchange of information.

Professor Michael Schmitt suggests the following criteria for analysis in accordance with international law: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility[12].

The basic principles contained in *The Hague Convention*, regarding the application of armed forces are those of military necessity, proportionality, humanity and chivalry. If a state's military is conducting cyber operations in accordance with these principles, it may be said to be engaging in a cyber-war.

Council of Europe's stance on cybercrime. In this context, *The Council of Europe Convention on Cybercrime* is the first international treaty that attempts to harmonise laws across countries as to what constitutes criminal activity in the cyber realm. This law enforcement treaty, also known as the *"Budapest Convention"*, requires signatories to adopt criminal laws against various types of activities in cyberspace, to empower law enforcement institutions to investigate such activities and to cooperate with similar agencies of other signatory states[13]. While it is widely recognised as the most substantial international agreement regarding cyber security, some observers consider it as unsuccessful[14]. Some critics warn that the Convention provisions are limited on the enforcement side and lacks corresponding legislation in all countries, so criminals can operate freely in this field. In addition, by September 2019, only 64 states have ratified it.

UN General Assembly resolutions relating to cyberspace. A series of UN General Assembly resolutions relating to cybersecurity have been adopted over the past 19 years. One resolution requested for the convening of a report from an international group of government experts from 15 states, including the USA. The stated goal of this process was to build a *"cooperation for a peaceful, secure, resilient and open ICT environment"* by reaching an agreement on the *"norms, rules and principles of responsible behaviour by States"* and identifying

[12] Katharina Ziolkowski, *"Ius ad bellum in Cyberspace – Some Thoughts on the <Schmitt-Criteria> for Use of Force"*, in *Legal & Policy Branch NATO CCD COE*, pp. 1-7, https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_ IusAdBellumInCyberspace.pdf, retrieved on 06.01.2020.

[13] *"Convention on Cybercrime"*, Budapest, 23.XI.2001, in *Council of Europe, European Treaty Series-No. 185*, pp. 7-13, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680081561, retrieved on 06.01.2020.

[14] Jack Goldsmith, *"Cybersecurity Treaties: A Skeptical View"*, 2 June 2011, in *Future Challenges in National Security and Law,* edited by Peter Berkowitz, pp. 1-11, http://media.hoover.org/sites/default/files/documents/Future Challenges_Goldsmith.pdf., retrieved on 06.01.2020.

capacity-building measures for confidence and capabilities, including for exchange of information. Unlike the work done in Tallinn under the auspices of NATO, this US-led process included both China and Russia. The resulting 2010 report, sometimes referred to as the *Group of Governmental Experts Report* recommended a series of measures to *"reduce the risk of misperception resulting from ICT disruptions"*, but did not include any binding agreements[15].

Nevertheless, some analysts consider that the report represents progress in overcoming differences between the USA and Russia regarding various aspects of cybersecurity. In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society, to discuss information society opportunities and challenges. This Summit was convened for the first time in Geneva, in 2003, and then in Tunis, in 2005, and then, after 10 years, in Geneva, in May 2013. Delegates from 175 countries attended the first Summit, where they adopted a *Declaration of Principles* – a road map for achieving an open information society. The Geneva Summit has left other, more controversial problems unresolved, including the issue of Internet governance and funding. At both summits, proposals for the USA to give up control of the *Internet Corporation for Assigned Names and Numbers* were rejected. An international treaty banning cyberwar and the use of information as a weapon was proposed at the UN by the Russian and German delegations.

Other international agreements regarding cyberwar. Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cyber security, for example, by prohibiting the disruption of air traffic control or other conduct that might jeopardise aviation safety[16]. Bilateral plans, mutual legal assistance treaties between countries may be applicable for criminal investigations in cyber security and prosecution.

In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society, to discuss information society opportunities and challenges. This Summit was convened for the first time in Geneva, in 2003, and then in Tunis, in 2005, and then, after 10 years, in Geneva, in May 2013. Delegates from 175 countries attended the first Summit, where they adopted a Declaration of Principles – a road map for achieving an open information society.

[15] United Nations Secretary-General, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"*, 30 July 2010, *United Nations General Assembly*, pp. 7-8, https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201, retrieved on 06.01.2020.

[16] Oona A. Hathaway, *op. cit*. pp.11, 28, 31-32.

CYBERTERRORISM – CHARACTERISTIC FEATURES

As with cyberwarfare, in most national laws or in international law, there is no consensus definition of what constitutes cyberterrorism. Some definitions addressing terrorist acts that transcend borders refer to some activities and damage defined in the fraud and abuse in networks and information systems. An important aspect of these legal documents is the approach regarding *"punishment for an offense"*, which entails fines or imprisonment and suggests that the aggressor party has committed a criminal act rather than an act of terrorism, while others claim it is an act of war, whether committed by a state actor.

For example, the USA considers it is illegal for an entity to *"knowingly access a computer without authorisation or exceeding the level of authorised access, and by means of such conduct having obtained information, that has been determined by the Government, pursuant to a law, to require protection against unauthorised disclosure for reasons of national security or foreign relations or are restricted from other reasons, with reason to believe that such information so obtained could be used to injury the USA or can be used to the advantage of any foreign state"*[17]. According to the FBI, the Internet and, in particular, the use of social media are among the key *"factors that have contributed to the evolution of the terrorism threat landscape"* since the terrorist attacks on 11 September 2001[18].

Some legal analyses define cyberterrorism as *"the premeditated use of disruptive activities or the threat thereof, against computers or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives"*[19]. However, these actions are also considered criminal and generally refer to individuals or organisations rather than to state actors. Some definitions of cyber terrorism focus on the distinction between the disruptive and destructive action, the terrorism generating fear comparable to that of physical attack

The USA considers it is illegal for an entity to "knowingly access a computer without authorisation or exceeding the level of authorised access, and by means of such conduct having obtained information, that has been determined by the Government, pursuant to a law, to require protection against unauthorised disclosure for reasons of national security or foreign relations or are restricted from other reasons, with reason to believe that such information so obtained could be used to injury the USA or can be used to the advantage of any foreign state".

17 H. Marshall Jarrett, *Prosecuting Computer Crimes*, in *Office of Legal Education Executive Office for United States Attorneys,* pp. 12-13, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ccmanual.pdf, retrieved on 06.01.2020.

18 FBI, *"Terrorism"* in *What We Investigate*, https://www.fbi.gov/investigate/terrorism, retrieved on 06.01.2020.

19 Barry C. Collin, *"Cyberterrorism"*, in *Institute for Security and Intelligence*, *11th Annual International Symposium on Criminal Justice Issues*, p.1, https://www.nato.int/structur/library/bibref/cyberterrorism.pdf , retrieved on 06.01.2020.

and is not just a costly disaster. Although a DDoS attack itself does not produce this kind of fear or destruction, the problem is the potential for second or third order effects. For example, if the telecommunications and emergency services were completely inoperable in a time of crisis, the effects of that sort of infrastructure attack could be catastrophic. However, in this case, the emergency service system itself is most likely not a target, but rather the result of collateral damage to vulnerable telecommunications network. Since the 2007 attack on Estonia, NATO has established authorities relating to cyber defence, with the goals of advancing strategy and centralising defence capabilities across members. A policy on cyber defence and an associated action plan were adopted in 2011, and to facilitate the centralisation effort, the NATO Communications and Information Agency was established in 2012[20].

Characteristics of cyberterrorism. In specialised literature for analytical and statistical purposes, there are various definitions for the term *"cyber terrorism"*, just as various definitions exist for the term *"terrorism"*. Terrorism has been defined as premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence a certain community. Dorothy Denning, security expert, defines cyberterrorism as *"... politically motivated hacking operations into networks and intelligence data, intended to cause grave harm, such as loss of life or severe economic damages"*[21]. The US Federal Emergency Management Agency defines cyberterrorism as *"unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives"*[22].

Others analysts indicate that a physical attack that destroys computerised centres for critical infrastructure, such as the Internet, telecommunications, or electricity power grid, ever touching

In specialised literature for analytical and statistical purposes, there are various definitions for the term "cyber terrorism", just as various definitions exist for the term "terrorism". Terrorism has been defined as premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence a certain community.

20 Olivier Kempf, *"NATO and Cyber Defense"*, in *NDC Research Paper*, article no. III.6, May 2013, p. 3, https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf , retrieved on 07.01.2020.

21 Dorothy Denning, *"Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy"* in *Nautilus Institute, Conference on "The Internet and International Systems"*, p. 3, https://www.rand.org/ content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf , retrieved on 06.01.2020.

22 Sarah Gordon, *"Cyberterrorism?"*, in *Symantec White Paper*, July, 2002, p. 4, https://www.symantec. com/avcenter/reference/cyberterrorism.pdf , retrieved on 07.01.2020.

a keyboard, can also contribute to or be labelled as cyberterrorism[23]. The proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. However, there are links between terrorist groups and criminals, that allow terror networks to expand internationally through leveraging the information resources, money laundering activities, or transit routes operated by criminals[24]. Some experts estimate that advanced or structured cyber-attacks, against multiple systems and networks, including targets surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyber-attack, causing mass disruption against integrated, heterogeneous systems, may require six to ten years of preparation[25].

There may also be the cases that individuals providing computers expertise to a criminal or terrorist may not be aware of the intentions of the individual that requested the support. In this context, it remains difficult to identify the sources responsible for most of the disturbing yet increasingly sophisticated attacks that compromise the Internet.

Analysis circumstances on cyber terrorism. Distinctions between crime, terrorism and war tend to blur when attempting to describe a computer network attack (CNA) in ways comparative to other areas of social life. For example, if a state were to secretly sponsor nonstate actors that initiate a CNA to support terrorist activities or to create economic disruption, the distinction between cybercrime and cyberwar becomes less clear, because it is difficult to say from where a cyber-attack originates, taking into account that an attacker may direct suspicion toward an innocent third party. Likewise, the interactions between terrorists and criminals who use ICT may sometimes blur the distinction between cyber-crime and cyber terrorism.

There may also be the cases that individuals providing computers expertise to a criminal or terrorist may not be aware of the intentions of the individual that requested the support. In this context, it remains difficult to identify the sources responsible for most of the disturbing yet increasingly sophisticated attacks that compromise the Internet.

[23] Edward V. Linden, *"Focus on Terrorism"*, in *Nova Science Publishers, Inc*, vol.9, p.6, https://books. google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+ Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+2003,+p.6&source=bl&ots= dRkvffLk4i&sig= ACfU3 U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4 sKHSzXB8wQ6AEw AH oECAoQAQ#v =onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism %E2 %80%9D%2C%20Computerworld%2C%20August%2011%2C%202003%2C%20p.6&f=false, retrieved on 07.01.2020.

[24] Rollie Lal, *"Terrorists and Organized Crime Join Forces"*, in *The New York Times*, May 24, 2005, p. 1, https://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html, retrieved on 07.01.2020.

[25] Clay Wilson, *"Computer Attack and Cyberterrorism"*, in *Naval History and Heritage Command*, p. 17, https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html, retrieved on 07.01.2020.

Given the difficulty in determining the author of the intrusion or the cyber-attacks, some argue that, unlike responding to traditional criminal acts, the focus should be placed on the act rather than the perpetrator and the threshold for triggering defensive or offensive action should be lowered. The Internet was used as a prime recruiting tool for insurgents in Iraq[26]. Insurgents have created many Arabic language websites that had the responsibility to contain coded plans for new attacks. Some reportedly give advice on how to build and operate weapons, and how to cross border checkpoints[27]. Other news articles report that a younger generation of terrorists and extremists, such those behind the July 2005 bombings in London, are learning new technical skills to help them avoid detection by law enforcement ICT[28].

When is cyber-attack considered cyber terrorism? Some analysts believe that the term *"cyber terrorism"* is inappropriate because a widespread cyber-attack may simply produce disarray, suffering, not terror, as would produce a bomb or other chemical, biological, radiological or nuclear weapon. However, some analysts believe that the effects of a widespread computer networks attack would be unpredictable and might cause enough economic disruption, fear and civilian deaths, to qualify as an act of terrorism[29].

It may highlight at least two points of view to define the term cyber terrorism: effects based:, intent based.

So, it may highlight at least two points of view to define the term cyber terrorism:

1. *effects based*: cyberterrorism exists when information attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if committed by criminals;

2. *intent based*: cyberterrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or certain personalities to promote a political agenda or to cause grave harm or severe economic damage.

Effectiveness of current legislation. Do the institutions in the field of security have the authority they need to effectively fight and win wars

[26] Jonathan Curial, *"Iraq's Tech-savvy Insurgents Are Finding Supporters and Luring Suicide-bomber Recruits over the Internet"*, in *San Francisco Chronicle*, 10 July 2005, pp. 1-3, https://www.sfgate.com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php, retrieved on 07.01.2020.

[27] *Ibidem*, p. 1.

[28] Michael Evans, Daniel McCrery, *"Terrorists Trained in Western Methods Will Leave Few Clues"*, in *London Times*, 12 July 2005. pp.1-3, https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q, retrieved on 07.01.2020.

[29] Serge Karsavina, *"What is Cyber-Terrorism?"*, in *Computer Crime Research Center,* p. 1, http://www. crime-research.org/analytics/Krasavin/, retrieved on 07.01.2020.

in cyberspace? Some analysts have argued that to fulfil the homeland defence mission, the institutions in the field of security should be given increased authority over private sector critical infrastructure protection. Yet business owners, particularly in the IT sector, contend that this would represent a *"militarisation of cyberspace"* that would create distrust among consumers and shareholders, and could potentially stifle innovation, leading to decreases in profits.

As highlighted, the international community must eliminate a certain amount of ambiguity regarding what constitutes an *"armed attack"* in cyberspace and what the thresholds are for a cyber-attack to be considered an act of war, an incident of national significance, or both. Without clear red lines and specific consequences articulated, deterrence strategies may be incomplete. On the other hand, a lack of red lines and consequences could constitute a form of strategic ambiguity that gives the institutions in the field of security operational manoeuvrability.

Most of defence, public order and national security institutions are supported partially by civilian high technology services and products, most often in the form of communications systems and computer software. A high percentage of military messages "flow" through commercial communications channels, and this reliance creates a vulnerability during conflict or a crisis situation.

CONCLUSIONS

Today, obviously, cyberspace have become another dimension, potentially for both cooperation and conflict. Concern regarding potential damage from cyberterrorism has grown as increasing amounts of economic activity occur online.

Most of defence, public order and national security institutions are supported partially by civilian high technology services and products, most often in the form of communications systems and computer software. A high percentage of military messages *"flow"* through commercial communications channels, and this reliance creates a vulnerability during conflict or a crisis situation. In future conflicts that involve cyberwarfare between states, the distinction between military and civilian targets may be blurred and civilian computer systems may increasingly be seen as viable targets vulnerable to attack by adversaries. Computer networking technology and information systems have also blurred the boundaries between cyberwarfare, cybercrime, and cyberterrorism. Officials in government and industry now say that cybercrime and cyberattack services available for hire from criminal organisations are a growing threat to the states national security as well as to their economy.

New and sophisticated cybercrime tools could operate to allow a state actor or terrorist group to remain unidentified while they direct

cyber-attacks through the Internet. It can be concluded that past incidents of conventional terrorism have already been linked with cybercrime, and that computer vulnerabilities may make government and civilian critical infrastructure systems seem attractive as targets for cyberattack. There are indications that suggest possible connections between cybercriminals and terrorist groups that want to damage a state economy or national security interests.

It is clear that terrorist groups are using computers and the Internet to further goals associated with spreading terrorism. This can be seen in the way that extremists are creating and using numerous Internet websites for recruitment and fund-raising activities, and for Jihad training purposes. Several criminals who have recently been convicted of cybercrimes used their technical skills to acquire stolen credit card information in order to finance other conventional terrorist activities.

The states experience difficulties in establishing the strategy for selecting and implementing an appropriate military or legally response after such an attack.

The states experience difficulties in establishing the strategy for selecting and implementing an appropriate military or legally response after such an attack.

Labelling a *"cyberattack"* as *"cybercrime"* or *"cyberterrorism"* is problematic because of the difficulty in determining with certainty the identity, intent, or the political motivations of an attacker.

Suggestions to increase incentives regarding cyber space security may include requiring that all software procured for national agencies should be certified, under the common criteria testing programme, which should also be a mandatory requirement for the software procurement, although the domain analysts point out that the software certification process is lengthy and may interfere with innovation and competitiveness in the global software market.

It may be suggested that the agencies operating national security systems are required to purchase software products from a list of lab-tested and evaluated products in a programme run by the institutions with responsibilities in security.

BIBLIOGRAPHY:

1. ***, *"Convention on Cybercrime"*, in *Council of Europe, European Treaty,* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680 081561.
2. ***, FBI, *"Terrorism"*, in *What We Investigate*, https://www.fbi.gov/investigate/terrorism.

3. ***, *"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"*, in *US Department of State*, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_ strategy_for_cyberspace.pdf.
4. ***, *Law no. 362/2018 on ensuring a common level of security of networks and information systems,* in the *Official Gazette,* Part I no. 21 of 9 January 2019.
5. *** *"National Strategy for Counterterrorism of The United States of America"*, in *The White House*, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.
6. ***, *"Significant Cyber Incidents Since 2006"*, in *Centre for Strategic & International Studies*, https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa.
7. ***, *"Tallinn Manual on the International Law Applicable to Cyber Warfare"*, in *The NATO Cooperative Cyber Defence Centre of Excellence*, http://csef.ru/media/articles/3990/ 3990.pdf.
8. ***, United Nations Secretary General, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"*, *United Nations General Assembly*, https://www.un.org/ga/search/view_ doc.asp?symbol=A/65/201.
9. Barry C. Collin, *"Cyberterrorism"*, in *Institute for Security and Intelligence*, *11th Annual International Symposium on Criminal Justice Issues*, https://www.nato.int/structur/ library/bibref/cyberterrorism.pdf.
10. Jonathan Curiel, *"Iraq's Tech-savvy Insurgents Are Finding Supporters and Luring Suicide-bomber Recruits over the Internet"*, in *San Francisco Chronicle*, https://www.sfgate. com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php.
11. Dorothy Denning, *"Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy"*, in *Nautilus Institute,* Conference on *"The Internet and International Systems",* https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.
12. Michael Evans, Daniel McGrory, *"Terrorists Trained in Western Methods Will Leave Few Clues"*, in *London Times*, https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q.
13. Jack Goldsmith, *"Cybersecurity Treaties: A Sceptical View"*, in *Future Challenges in National Security and Law",* http://media.hoover.org/sites/default/files/documents/ Future Challenges_ Goldsmith.pdf.
14. Sarah Gordon, *"Cyberterrorism?"*, in *Symantec White Paper*, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

15. Oona A. Hathaway, *"The Law of Cyber-Attack",* in *California Law Review,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.
16. Jarrett H. Marshall, *"Prosecuting Computer Crimes"*, in *Office of Legal Education Executive Office for United States Attorneys,* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual. pdf.
17. Olivier Kempf, *"NATO and Cyber Defense"*, in *NDC Research Paper*, https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf.
18. Harold Hongju Koh, *"International Law in Cyberspace"*, in *US Department of State*, *Archived content*, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
19. Serge Krasavin, *"What is Cyber-Terrorism?"*, in *Computer Crime Research Center,* http://www. crime-research.org/analytics/Krasavin/.
20. Rollie Lal, *"Terrorists and Organized Crime Join Forces"*, in *The New York Times*, https://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html.
21. Edward V. Linden, *"Focus on Terrorism"*, in *Nova Science Publishers, Inc*, https://books.google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+2003,+p.6&source=bl&ots=dRkvffLk4i&sig=ACfU3U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4sKHSzXB8wQ6AEwAHoECAoQAQ#v=onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism%E2%80%9D%2C%20Computerworld%2C%20August%2011%2C%202003%2C%20p.6&f=false.
22. Barak Obama, *"Remarks by the President in Year-End Press Conference"*, in *The White House Office of the Press Secretary*, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.
23. Chris Strohm, *"FBI Provides More Proof of North Korea Link to Sony Hack"*, in *Bloomberg*, https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony.
24. Clay Wilson, *"Computer Attack and Cyberterrorism"*, in *Naval History and Heritage Command*, https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html.
25. Katharina Ziolkowski, *"Ius ad bellum in Cyberspace – Some Thoughts on the ‹Schmitt-Criteria› for Use of Force"*, in *Legal & Policy Branch NATO CCD COE*, https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf.

SECURITY OF INFORMATION AND OF MILITARY INFORMATION SYSTEMS

Colonel (ret.) Professor Gheorghe BOARU, PhD

Full member of the Academy of Sciences of the National Security,
Full member of the Academy of Romanian Scientists,

Colonel Iulian Marius IORGA, PhD

Ministry of National Defence

The way of approaching the field of information security and military information systems is based on the fact that Romania is a NATO member and that, in joint military actions, it uses information systems that must be compatible and interoperable, but also protected.

From the informational point of view, in the military actions there is a fight for information, through information and against information and therefore its security is a special activity, particularly with a view to classified information.

The Alliance members, including Romania, must provide, individually or through bilateral cooperation agreements, the protected information resources, both as a process and as a system, necessary to fulfil the joint operations' objectives under NATO command.

Most of the informational threats come through virtual space. In this sense, it is considered that the security of the virtual space has become one of the most pressing security challenges of the 21st century.

Keywords: information, information system, vulnerabilities, threats, risks, cyber security.

INTRODUCTION

In order to fulfil the missions that respond to the new challenges of the security environment, the Romanian Armed Forces have engaged in a broad transformation process established in the *Romanian Armed Forces Transformation Strategy*[1].

In this sense, by 2025, the transformation process is planned to undergo the following three phases[2]:

- **the basic restructuring** (2005-2007);
- **NATO and EU operational integration** (2008-2015),
- **full NATO and EU technical integration** (2016-2025).

The third phase will ensure achievement of long-term transformation objectives: efforts, as well as financial and human resources will be focused on providing the capabilities assumed and included in the capability targets and on participating in NATO and EU – leading missions and operations; going on with improving and outfitting with new equipment and reaching the interoperability level with other EU and NATO armed forces etc.

In this context, the basic objective of the transformation process is to adjust the structure of the Romanian Armed Forces to the present and future security environment, in order to fulfil the national commitments to the Alliance, concordant with the processes and phenomena in the NATO transformation plan.

The basic objective of the transformation process is to adjust the structure of the Romanian Armed Forces to the present and future security environment, in order to fulfil the national commitments to the Alliance, concordant with the processes and phenomena in the NATO transformation plan.

The aim is to make the Romanian Armed Forces able to participate in the entire spectrum of missions carried out by the Alliance and the EU.

I consider this the legal context in which the Romanian Armed Forces can develop the military actions, actions in which the command and control processes are based on the specific information processes.

[1] *Strategia de transformare a Armatei României*, Bucureşti, 2007.

[2] See https://fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/, retrieved on 20 February 2020.

MILITARY INFORMATION AND ITS SECURITY

Thorough information is well known to result in an efficient command and control process.

In our armed forces, the intelligence support to operations is well regulated, representing the *"basic form of assuring the actions and the force protection, and establishing the set of measures and actions, continuously and unitarily carried out by all the participating forces and at all levels in order to plan, obtain, verify, process and capitalise on the data and the intelligence regarding the situational factors"*[3].

In our armed forces, the intelligence support to operations is well regulated, representing the "basic form of assuring the actions and the force protection, and establishing the set of measures and actions, continuously and unitarily carried out by all the participating forces and at all levels in order to plan, obtain, verify, process and capitalise on the data and the intelligence regarding the situational factors".

The field literature approaches information both as *"a powerful weapon and as a preferred target"*[4], or it is stated that *"information can be the most feared weapon in the technological developments of the battlefield"*[5].

If this information is correlated with other information already known and if it is analysed from the past experiences' perspective (collation and processing), they emerge in a new set of meanings with a different informational value, a process called *"intelligence"*.

By studying the relationship between data, information and intelligence, we can conclude that the processed information is transformed into intelligence products, which are obtained as a result of a structured process, called in the NATO doctrines or those of allied states, *the intelligence cycle*.

We assess that, in the case of NATO multinational joint operations, *"intelligence"* does not mean *"information"*, but a complex process determining the enemy's intentions and most likely course of action.

Within the basic systems and processes involved in the multinational joint operation planning – *intelligence* can have the attribute of[6]: combat function; combat ability; cycle; process and system.

[3] I.P.S.-3.1, *Manualul privind procedurile de informaţii militare pentru sprijinul operaţiilor*, SMG, Bucureşti, 2006, p. 14.

[4] *Cornerstones of Information Warfare,* Department of the Air Force, Washington DC, 1995, p. 2.

[5] Peter Grier, *Information Warfare,* Air Force Magazine, No. 3, March 1995, p. 23.

[6] Colonel (r.) Professor Dr Gheorghe Boaru, Colonel, doctoral student, Iulian-Marius Iorga, *Ciclul informațional ca proces, procesul și ciclul "Intelligence" – în cadrul acțiunilor militare moderne,* Revista de Științe Militare, published by the Academy of Romanian Scientists, no. 1, 2017, pp. 84-85.

In analysing the intelligence process, we take as a reference the NATO Doctrine for Intelligence[7], because to this are compared the intelligence aspects analysed in the NATO Forces activity, in allied states' Armed Forces, as well as in those forces' intelligence doctrines[8].

In order to achieve the intelligence requirements, intelligence structures adapted to the new realities of the operational environment are needed, based on a training process that will allow them to successfully tackle the challenges related to applying the new Allied concepts: *"hybrid operations"*, *"comprehensive approach"*, *"information sharing"*, *"need to know vs. need to share"*.

In order to achieve the intelligence requirements, intelligence structures adapted to the new realities of the operational environment are needed, based on a training process that will allow them to successfully tackle the challenges related to applying the new Allied concepts: "hybrid operations", "comprehensive approach", "information sharing", "need to know vs. need to share".

According to the opinion of some Romanian military specialists[9], in order to integrate the intelligence activities under a single name, the NATO member states' armed forces have standardised the ISTAR concept (Intelligence, Surveillance, Target Acquisition and Recognition). The same authors also specify that different ISTAR acronym variants are used, such as: STAR, RSTA, STA, ISR, exclusively to highlight partial information activities.

In the Romanian Armed Forces, according to the *Doctrine for Intelligence, Counterintelligence and Security of the Armed Forces*, the ISTAR[10] concept has been accepted and integrated in the specific national norms as an *"organisational solution, meant to functionally integrate all the available collection capabilities, normatively defined, under the circumstances of using a set of actions, procedures, measures and resources (technical, human, financial etc.)"*[11]. This concept has been normatively designed to provide *the connection between collection, processing and dissemination of data and intelligence in order to support the commander in reaching the operational objectives in the conflict spectrum*[12].

[7] AJP-2, *The Allied Doctrine for Intelligence, Counterintelligence and Security,* 2003.

[8] *Doctrine for Intelligence Support to Joint Operations* (of the Romanian Armed Forces, A.N.), 2003; *Doctrine for Intelligence in Joint Operations* (of the Canadian Armed Forces, A.N.), 2003; JDP 2-00, *Understanding and Intelligence Support to Joint Operations* (of the UK Armed Forces, A.N.), 2011; JP-2, *Intelligence in Joint Operations* (of the US Armed Forces, A.N.), 2007.

[9] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale militare – servicii şi tehnologie*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2010, pp. 24-25.

[10] *Ibidem.*

[11] *Doctrina pentru Informaţii, Contrainformaţiişi Securitate a Armatei*, Bucureşti, 2005, p. 34.

[12] *Ibidem*, p. 35.

The fact that there is such a normative and enforcement capacity in the military intelligence field, at the Romanian Armed Forces level, shows that the essence of the information support integrating efforts concept is to use all the possibilities offered for this field in an integrated environment, thus allowing the Romanian procedural environment integration with that of other NATO member states.

In this informational normative context, the security of information and military information systems is mandatory, so it requires knowledge and concern for this field, as well as establishing the most effective measures.

Therefore, we consider that, in the context of Romania's NATO membership, and in the perspective of adapting and transforming Romanian doctrinal and action approaches, the staff officers' concern to know and address the problem of information security according to the Alliance's demands is justified.

Modern armed forces pay special attention to this problem, considering it a key objective for winning the information battle, whose foundation is represented by the introduction, on an extended scale, of information technology and of the modern means of communication and information technology, in the whole space of the battlefield.

We also consider particularly important the aspects related to the classified information which requires protection against unauthorised disclosure and which carries specific identifiers, as well as non-classified information that is not intended for public use and is protected by internal measures specific to each organisation, as well as information of public interest, respectively that information which concerns or results from activities carried out by a public authority or public institutions.

Furthermore, measures for the protection of information against dangers and threats specific to the informational age are presented in the NATO and the Allied armed forces regulations and military handbooks.

In accordance with Law no. 182/2002, the Government Decision no. 585/2002 regarding the National Standards for the protection of classified information was issued. At the same time, the equivalence levels of the classified information from Romania with those

from NATO and/or the EU have been established, as shown in the table below.

Table no. 1

Levels of Equivalence in Romania – NATO – the EU[13]

Romania – classified information		NATO – classified information	The UE – classified information
Secret de stat	Strict secret de importanţă deosebită/SSID	NATO TOP SECRET/ NTS	TRÈS SECRET UE/TSUE
	Strict secret/SS	NATO SECRET/NS	SECRET UE/SUE
	Secret/S	NATO CONFIDENTIAL/NC	CONFIDENTIEL UE/ CUE
Secret de serviciu/SSv		NATO RESTRICTED/NR	RESTREINT UE/RUE

NATO information security[14] is ensured according to Law no. 423/2004, and, through the Government Decision no. 353/2002, the Norms regarding the protection of the classified information of the North Atlantic Treaty Organisation in Romania are established.

In this context, we consider that information security is a field whose importance is constantly increasing and which must be approached from all possible angles, starting from concepts, vulnerabilities, risks, and management.

SECURITY OF MILITARY INFORMATION SYSTEMS

In order to function, military organisations use information systems. The more complex they are, the more information they need. Therefore, the informational component of any system is constantly growing and diversifying, and the lack of information determines its disappearance.

Consequently, those information systems must be designed so that they are efficient and their security is assured in any situation. Only in this way can the security, accuracy and timeliness of the information necessary for the command and control process can be ensured, as a key component of military actions.

In order to function, military organisations use information systems. The more complex they are, the more information they need. Therefore, the informational component of any system is constantly growing and diversifying, and the lack of information determines its disappearance.

[13] Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne,* Editura Universității Naționale de Apărare *"Carol I"*, București, 2018, p. 93.

[14] Law no. 423/2004 on Romania's Accession to the NATO Agreement on Information Security, adopted in Brussels, on 6 March 1997.

As specificity of the military field, the importance of the information systems continuously increases, achieving symbiosis with the command and control processes, functioning cohesively and rendering higher quality to the management of the organised and/or carried out actions.

Command and control activities, specific to the military field, but particularly, the effective conduct of military actions, the military entity's ability to successfully carry out a mission are influenced by the data and information needs, as well as by the ability to obtain the informational advantage, determined by the available information capabilities and the security of the informational-decision-making system.

As specificity of the military field, the importance of the information systems continuously increases, achieving symbiosis with the command and control processes, functioning cohesively and rendering higher quality to the management of the organised and/or carried out actions.

The concept of information system has been studied by specialists from different fields of activity, from the perspective of both its structure and its functioning, but no single definition has been reached.

The structure of the information system depends on its destination, on the complexity and the spatial distribution of the command and control elements assisted, as well as on its objectives and processes.

Different categories of information systems have been studied, such as security and national defence, technical, social, economic etc. systems, among which there are important dissimilarities and which have common structure elements, but also specific elements, which shape the difference.

We can consider that the structure represents the organisational component, which defines the systemic conception and allows an information system to be made up of modules (subsystems). This can be done by identifying, grouping, arranging and optimally interconnecting the infrastructure and management elements, also taking into account the technical resources, the databases, the software components and, essentially, the security elements.

A thorough informational assurance of the organisational structures, in which the command and control and the operational activities (of execution) are well defined, can be a favourable premise for the mission success.

In the military organisation, the structure of the information system is determined and basically depends on the structure of the command and control system. Between the two structures, there is a mutual, shared, interdependence.

Studying and analysing several **definitions of the information system**[15], presented in specialised military and/or civilian Romanian and/or foreign papers, we found that all are based on structural, technical, functional and management elements specific to the field addressed.

We present here five of the most significant definitions mentioned in the specialised literature, above-referred, in which the information system:

1. *"is a system of persons, data records and activities on data and information processing within an organisation, including processes of manual or automatic processing thereof. Information technology is a key component of the information system"*[16];

2. *"represents the integrated set of components for information collecting, storing, processing and communicating. Its main elements are: computers (hardware), software, databases, communication systems, human resources and procedures"*[17];

3. *"represents a set of equipment, methods and procedures and, if necessary, personnel organised to perform the functions of information processing"*[18];

4. *"includes the entire infrastructure, circuits and information flows, organised in a unitary conception, the personnel, all the components that collect, transmit, store, process, elaborate/process information and ensure their display and dissemination, in order to use them in the management process (command and control) and in carrying out military actions"*[19];

---

[15] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare,* Editura Universității Naționale de Apărare *"Carol I"*, București, 2018.

[16] *Information Systems*, Wikipedia, the free encyclopaedia, http:/en.wikipedia.org/ wiki/ Information Systems, retrieved on 20 March 2020.

[17] *Britannica Encyclopaedia*, http://www.britannica.com/EBchecked/topic/287895/ Information Systems, retrieved on 20 March 2020.

[18] AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008, p. 2-I-4.

[19] FM 101-5-1, *Terms and Operational Symbols, Land Forces General Staff*, USA.

5. *"includes the entire infrastructure, organisation, personnel and components for collecting, processing, storing, transmitting, displaying, disseminating and acting on information"*[20].

Referring to **the management information system** (MIS), centred on managerial objectives, an interesting approach has the following two definitions:

1. *"The managerial information system (MIS) consists of all the data, information, flows and information circuits, procedures and means of information processing, meant to contribute to the establishment and achievement of the organisation's objectives"*[21].

2. MIS is defined as a *"combination of human and computer resources that aim at collecting, storing, organising, calling, communicating, distributing and using the data and information that managers use in exercising their management functions, in order to achieve efficient management. These systems provide direct, online access to the relevant information stored, friendly interface, in an easy-to-use dialogue"*[22].

Analysing the above definitions, it turns out that both essential components are highlighted, as well as certain features of the information system, each of which requires, in our opinion, certain additions, clarifications and updates.

Three specialists from *"Carol I"* National Defence University, taking into account the current achievements in the field and synthesising the opinions of different specialists, formulated the following general definition: "*the information system represents the integrated set of data, information and knowledge necessary for the organisation, mainly managed electronically, together with information infrastructure ...."*[23].

The management information system – MIS is defined as a "combination of human and computer resources that aim at collecting, storing, organising, calling, communicating, distributing and using the data and information that managers use in exercising their management functions, in order to achieve efficient management. These systems provide direct, online access to the relevant information stored, friendly interface, in an easy-to-use dialogue".

[20] US Army Field Manual 100-6, *Information Operations*, 1996; JP-02, DoD Dictionary of Military Terms, 2008, p. 261.

[21] Ovidiu Nicolescu et al., *Sistemul informaţional managerial al organizaţiei*, Editura Economică, Bucureşti, 2001, p. 25.

[22] Club IT&C, *Cum să exploatezi informaţia în mod inteligent-Management Information Systems*, https://www.google.ro/Club+IT%26C, +Cum+s%C4%83+exploatezi+informa%C5%A3ia +%C3%AEn+ mod+inteligent-Management+Information+ Systems&tbm..., retrieved on 1 February 2020.

[23] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale – fundamente teoretice –*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2009, pp. 194-195.

According to the same authors, unlike other opinions, the information infrastructure includes, besides *the information and communication technology*, *the specialists* in the field, as well as the *information management structure*.

In line with the same approach, it is envisaged that the information system will provide the data and information necessary for the command and control process, in order to optimally achieve the stated objective or mission and to obtain *competitive advantages*[24]. *The competitive advantage* is a critical mass synthesis of the relative advantages in the following fields: information, knowledge, understanding and decision-making (command and control), also including moral and leadership qualities.

Specifically, *the military information system*[25] is a large, dynamic, complex system, made up of several interdependent systems (which, hierarchically, are subsystems), that must be singularised, with a high degree of automation and self-regulation, managed in a centralised way. It is, in fact, a super-system (federation of systems), which comprises a homogeneous set of interconnected networks, together with their integrated elements for management, having the necessary inputs, internal structure and outputs, being characterised by a high degree of autonomy and heterogeneity.

The C4ISR/C5ISR-D systems involve the provision of information and knowledge to the political-military decision-makers in order to ensure a higher situational awareness. Given that military operations will be conducted with greater precision than ever, the mission effectiveness will increasingly depend on C4ISR/C5ISR-D systems, which are complex subsystem networks.

The military information system represents the dynamic side of the command and control (management) system of which it is a part, which provides optimal decision making, its functioning and cohesion, a reason for which, in some specialised works, it is called information-decision-making system or, in Western literature, managerial information system[26].

ROMANIAN MILITARY THINKING

The military information system is a large, dynamic, complex system, made up of several interdependent systems (which, hierarchically, are subsystems), that must be singularised, with a high degree of automation and self-regulation, managed in a centralised way. It is, in fact, a super-system (federation of systems), which comprises a homogeneous set of interconnected networks, together with their integrated elements for management, having the necessary inputs, internal structure and outputs, being characterised by a high degree of autonomy and heterogeneity.

[24] D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington DC, CCRP - Data publication, August 2001, p. 41.

[25] W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, EdituraTehnică, Bucureşti, 1970, p. 227.

[26] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale, op. cit.*, p. 195.

"*The information-decision-making system represents a cybernetic system, organised in a pyramid, in reciprocal, vertical and horizontal flows, based on a unitary mechanism for collecting and processing information, from the lowest hierarchical level to the highest, which allows for decision foundation, adoption and follow-up. This system ensures the implementation of the decision package and monitoring the effects of its application for the fulfilment of the organisation's objectives*"[27].

The information system includes the status information (reports, information, proposals, syntheses, notices, ...) coming from the execution bodies, various information sources, sensor systems, elements with which to cooperate or collaborate and goes out the control information (orders, provisions, specifications, indications, guidelines, ...) produced by the control units.

The information system not only contains technical elements but it is constituted as a complex set of specialised people as well as practical activities, technical equipment for collecting information (including through sensors), communications, storage, processing and display of information, software, databases and procedures, focused on identifying the information needs and the ways of fulfilling them, for the informational assurance of the management processes (command and control), including the decision transmission to the subordinate operational levels (echelons).

In another approach, *"The information system is the link between the command and control system and the operational (execution) system, which contributes to the symbiosis (approach), strengthening the discipline and increasing the responsibility for the activities carried out. It should not only be considered as an interface between these systems, but also as an element of connection between the internal information environment of the organisation (the military structure) and the external one through which almost all the necessary data and information are obtained"*[28].

The information system includes the status information (reports, information, proposals, syntheses, notices, ...) coming from the execution bodies, various information sources, sensor systems, elements with which to cooperate or collaborate and goes out the control information (orders, provisions, specifications, indications, guidelines, ...) produced by the control units.

[27] Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informaţională şi protecţia informaţiilor*, Editura Detectiv, Bucureşti, 2006, p. 71.

[28] Vasile Dumitru et al., *Sisteme informaţionale militare*, Editura CERES, Bucureşti, 2000, p. 38.

Regarding the role of the information system, analysed in close correlation with its place within the organisation (the military structure), we can assess that it consists of:

- determining the volumes of required data, information and knowledge, so that the decision-making and execution processes of the military structure have optimal performance;
- allowing to determine the sources that can obtain the information;
- establishing the technical means, which will ensure the information flows circulation and the information means for the information processing;
- establishing the information resources (data, information), circuits and information flows to be ensured. *Information resources* consist of information together with personnel, technical equipment and information technology;
- ensuring the specific informational functions (the activities of collecting, transmitting, storing, processing and disseminating information operatively), necessary for the command, control (management) and execution of the activities;
- ensuring the qualitative parameters necessary for the information (objectivity, opportunity, precision, integrity, relevance, authenticity) for the organisation command and control systems (military structure);
- applying effectively security policies, targeting both information and information processes.

ROMANIAN MILITARY THINKING

The safe and uninterrupted functioning of the information systems, which entirely depends on the organisational, technical and functional measures adopted, is a vital necessity for any organisation (military structure). Affecting, even partially, the work of the structural elements and their equipment (hardware, software), causes serious informational damage, by interrupting or delaying the command and control processes (management) as well as the operational ones (executional).

The safe and uninterrupted functioning of the information systems, which entirely depends on the organisational, technical and functional measures adopted, is a vital necessity for any organisation (military structure). Affecting, even partially, the work of the structural elements and their equipment (hardware, software), causes serious informational damage, by interrupting or delaying the command and control processes (management) as well as the operational ones (executional).

The use of information and communication technology has created the possibility of developing modern information systems, in which computer networks and communications have a decisive

role, but which also have significant vulnerabilities. At the same time, they are also subject to informational threats, due to the action of internal factors, but particularly external ones, which aim at limiting or interrupting the activities of information collecting, transmitting, processing and disseminating, for abnormal functioning or even blocking the system's functions.

Many of these threats come through virtual space. In this sense, it is considered that *"Securing virtual space has become one of the most pressing security challenges of the 21st century, due to its importance for daily life, for government, national security, business, as well as for citizens. The cyber world and associated technologies have created, on the one hand, more social, cultural, economic and political opportunities for all, and on the other hand, its borderless nature has brought with it threats such as cyber-attacks and cybercrime"*[29].

Essential questions about information network security: *"Who? When? Where from? What? Why?"* determine together a new phrase, *"of the five W's"* (*5W – Who, When, Where, What, Why?*). Who accesses the network? When and where does access occur? What information is accessed and why? These aspects must be monitored and secured, depending on the importance of the information, on the public or private character of the communications and information networks, regardless of the terminal used.

Internet connection is a facility, but most of the time, it creates major security issues for these networks, by creating breaches that can be accessed in an unauthorised way. The security services in the field of communications and information networks are aimed, on the one hand, at keeping them in operation, and on the other hand, at ensuring the security of the applications, as well as of the information stored on the storage base or transmitted through the network.

Internet connection is a facility, but most of the time, it creates major security issues for these networks, by creating breaches that can be accessed in an unauthorised way. The security services in the field of communications and information networks are aimed, on the one hand, at keeping them in operation, and on the other hand, at ensuring the security of the applications, as well as of the information stored on the storage base or transmitted through the network.

First and foremost, the security of these networks is ensured through strategies and doctrines, as well as through developing a security culture at national and European level.

[29] Colonel (ret.) Professor Dr Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, published by the Academy of Romanian Scientists, no. 2, 2018, p. 51.

We believe that these strategies must be applied both at European and national level. Thus, it is estimated that *"Improving the way the EU ensures cyber security is essential in order to continue to ensure the social, economic, financial and cultural benefits that citizens and businesses obtain from the Internet and, in a broader sense, the communications and information technology development. Moreover, it is essential for the EU to reach the goals it has set in the Digital Agenda for Europe (2010), and equally significant, the driving force of such an agenda – the Europe 2020 Strategy"*[30].

Fully concordant with the European actions, at the national level, the *National Strategy on the Digital Agenda for Romania 2020* was approved in February 2015[31].

This strategy *"defines four areas of action, of which only the first domain is worth mentioning here, namely: e-Governing, Interoperability, Cyber Security, Cloud Computing and Social Media. This document has taken over and adapted the elements of the Digital Agenda for Europe to the specificity of our country. The Digital Agenda thus defines the key role that ICT use must play in achieving the Europe 2020 goals"*[32].

The military information systems, such as C4I (C4I2, C4ISR, C5ISR, ...), a topical concept in European and Euro-Atlantic military theory and practice, integrate the command, information, communication and information subsystems, being based on doctrines and specific procedures, flexible structures, state-of-the-art equipment and, first and foremost, highly professional staff.

The military information systems, such as C4I (C4I2, C4ISR, C5ISR, ...), a topical concept in European and Euro-Atlantic military theory and practice, integrate the command, information, communication and information subsystems, being based on doctrines and specific procedures, flexible structures, state-of-the-art equipment and, first and foremost, highly professional staff.

In principle, any state or non-governmental organisation with hostile intentions may have the financial resources and the technological capacity to threaten a C4I system. Due to the low cost of the equipment needed for various forms of information attack, compared to the funds needed to develop a C4I system, as well as due to the fact that most of the knowledge required is freely spread around the world, threats can arise, including from terrorist groups or hackers.

[30] Colonel (r.) Professor Dr Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, no. 2, 2017, p. 71.

[31] The *National Strategy on the Digital Agenda for Romania 2020* was approved through Government Decision no. 245/7 April 2015.

[32] Colonel (r.) Professor Dr Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană, op. cit.*, p. 72.

Such attacks can be carried out for the purpose of disinformation, electronic espionage to obtain the global competitive advantage, clandestine change of sensitive data in the theatres of operations or for altering or interrupting the functioning of national critical infrastructures, such as those of energy, water, fuel, communications, banking or transport, which are essential for the society and economy functioning.

"At the military level, they can track sabotage, subversion, espionage or terrorism and are materialised in information leak exploitation/triggering, prevention of missions, inconsistencies in the course of operations"[33].

In Romania, the general cooperation framework that brings together those authorities and public institutions with responsibilities and competences in the cyber security field is represented by the National Cyber Security System (NCSS). The NCSS activity is coordinated at strategic level by the Supreme Council for the Country's Defence.

"The common feature of confrontations in the cyber space is the continuous antagonistic relationship established between the threats that arise in the cyber space – terrorism, espionage, sabotage, subversion and organised crime, on the one hand, and information security, on the other hand. These threats are manifested in a very wide environment, provided by the information warfare, in a sharp conceptual and action interference between the electronic warfare, the hackers, the psychological warfare, economic warfare and in a complex typology of the cyber-attacks"[34].

To conclude, in the current information age, technological security is of particular importance and also concerns the computer networks (COMPUSEC) and the communication networks (COMSEC).

We consider that the specific threats to cyber security, which have become more and more serious lately, are also due to the fact that they are not limited by borders and they register a permanent increase in frequency and sophistication as well as to the universal belonging of the cyber space. The security risks involved in cyber-attacks

The specific threats to cyber security, which have become more and more serious lately, are also due to the fact that they are not limited by borders and they register a permanent increase in frequency and sophistication as well as to the universal belonging of the cyber space. The security risks involved in cyber-attacks and the global nature of their effects require joint international cooperation efforts to ensure the security of the information systems of the Alliance members.

[33] Colonel (ret.) Professor Dr Gheorghe Boaru, *Război și apărare în spațiul virtual*, *op. cit.*, p. 54.
[34] *Ibidem,* pp. 54-55.

and the global nature of their effects require joint international cooperation efforts to ensure the security of the information systems of the Alliance members.

❖ **Vulnerabilities.**

As in any other field of activity, in the area of information and information systems as well, there are certain vulnerabilities, i.e. *"weak parts and weaknesses of the system, infrastructure, control environment or network design, which are not generated by the actions of the adversaries, but by their own solutions adopted, which can be attacked and exploited relatively easily, to damage the integrity of that system"*[35].

From a technical point of view, the vulnerability is presented as a system's feature, which can cause precise degradation to the system (the inability to perform its designed functions), as a result of being subjected to a precise level of effects, in an unnatural hostile environment.

In information operations, *vulnerability* is defined as a weakness in the information security system design, procedures, implementation or internal control, which can be exploited to gain unauthorised access to information or the information system. In communications and information systems, the vulnerability is represented by a point where a system is likely to be attacked. Any computer or with a significant degree of computerisation system is vulnerable to attack.

In the military information systems, we notice the much higher weight of those specific to computers and computer networks. This weight is explained both by the fact that, in the current information systems, the subsystem of computers has a systemic integrating role, and by the fact that the communication subsystem is, in its most important elements, computerised.

At the same time, it should be highlighted that both the hardware components (workstations, network wiring etc.) and the main

From a technical point of view, the vulnerability is presented as a system's feature, which can cause precise degradation to the system (the inability to perform its designed functions), as a result of being subjected to a precise level of effects, in an unnatural hostile environment.

[35] *Noul dicționar universal al limbii române*, Editura Litera Internațional, București-Chișinău, 2006, p. 1645.

software (operating systems) used are of civil origin, which results in the following disadvantages, from the security point of view:

- many of these are available to the general public, so their technical characteristics are known in detail by the potential adversary;
- the components produced especially for the military system, which, although designed and manufactured under the security conditions established and monitored by the military system, can nevertheless be subject to the actions of industrial espionage, a phenomenon specific to the aggression of the high technology free market and the IT market, in particular;
- the respective components allow for a reduced personalisation, so the results of a vulnerability study on the civil systems can be applied, to a large extent, also to the military ones;
- there are, in overwhelming proportion, imported components or, under best circumstances, produced and verified outside the military sphere, intentionally and very well camouflaged;
- the military systems are based on a logical component – the software one – which can also be attacked by logical means, therefore means that do not require expensive technologies, their range being continuously diversified by the contribution of the informational criminals.

With regard to the field of communications and information systems, the vulnerability is represented by a point where a system is likely to be attacked. Any information system, which has a significant degree of computerisation, is vulnerable to a variety of forms of attack.

Therefore, it is intended that the modern technology in the information systems to be tackled also with advanced technology, confirming the conclusion of the specialists that, in the future military conflicts, the greater the advantage obtained from the information and communications technology, the more it will increase its potential vulnerability.

It can be concluded that the main objective of contemporary military conflicts should not particularly materialise in the total destruction of the technique, armament or living force of the adversary, but especially in neutralising and disintegrating its complex systems, mainly information systems.

With regard to the field of communications and information systems, the vulnerability is represented by a point where a system is likely to be attacked. Any information system, which has a significant degree of computerisation, is vulnerable to a variety of forms of attack.

Besides the specific, external, internal vulnerabilities, the *"human errors"* type are not to be neglected.

Security policies and products can reduce the chances and likelihood for an attack to penetrate the computer system or, through the adopted security architecture, may require the aggressor to invest so much time and other resources that the attack will no longer be profitable.

Experts from around the world unanimously agree that there are no fully secure systems, so vulnerabilities are present even in the most advanced systems.

❖ **Threats**

A *threat* is a potential danger to the system. The danger may be represented by a person (a system cracker), a material element (an imperfect technical equipment component, for example) or an event (natural disasters, fires etc.), which may exploit a system vulnerability.

Covert threats are: espionage, sabotage, subversive acts, terrorism, acts that make up the specific crime.

Threats are analysed in relation to events that may occur as a result of their activity, events called attacks, as well as vulnerabilities that can be exploited by them.

The specialised literature classifies the sources of threats according to several criteria, as described below.

According to the manifestation mode, the sources of threats can be:

- manifest or open, in sight, these being observable;
- covered, masked or conspired;
- accidental and natural.

Visible threats are: radio jamming, radio broadcasting or radio navigation; electromagnetic pulse (EMP); SIGINT activities; special operations.

Covert threats are: espionage, sabotage, subversive acts, terrorism, acts that make up the specific crime.

Visible threats are: radio jamming, radio broadcasting or radio navigation; electromagnetic pulse (EMP); SIGINT activities; special operations.

Accidental and natural threats are classified as follows:

- natural: lightning, floods, earthquakes, extreme temperatures, strong wind;
- accidental: human errors, software errors, as well as hardware failures;
- fires, water leaks, dangerous voltages in the supply network.

According to their origin, the sources of threats can be: from the inside, from the outside or from the environment.

Within the planned information aggression, the possible threats to the military information systems come from all three types of sources.

When a message is transmitted through a communication channel, there are many general, voluntary or accidental threats.

❖ **Risks**

As a general approach within the military domain[36], the *risk* is defined as the probability and severity of a loss, related to the existence of dangers. Distinctly, the risk is seen as a limit, a maximum threshold for which a countermeasure established by norms has been shown to be effective in eliminating a vulnerability, in correlation with a given level of susceptibility and threat.

The risk defines an indicator, which represents the probability and the rate of occurrence of an event or action that, whenever occurring, causes the information itself or the material support of the information to deteriorate.

The risk defines an indicator, which represents the probability and the rate of occurrence of an event or action that, whenever occurring, causes the information itself or the material support of the information to deteriorate.

There is a directly proportional relationship between vulnerability and risk in relation to threats[37].

Given that we cannot influence threats in any way, implicitly not the probability of occurrence, the only way to reduce the risks is the leverage of action on the vulnerability, respectively the degree of vulnerability.

ATTACKS ON COMMUNICATIONS AND COMPUTER NETWORKS

Attacks on communications networks can be grouped according to certain criteria. Depending on where they are executed, the attacks can be: local or remote.

Local attacks materialise by compromising the security of a network by a local user.

[36] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare, op. cit.*, pp. 39-40.

[37] Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acțiunile militare,* Editura AÎSM, București, 2003, pp.17-25.

The risk of compromising the security of a network can be addressed (eliminated, diminished, distributed) in several ways:

- granting privileges strictly necessary to the local users, for the fulfilment of daily tasks, according to the tasks assigned in the job descriptions;
- network surveillance, in order to prevent possible attempts to breach the norms required to comply, including after the end of the working hours;
- access restriction to important network equipment;
- balanced distribution of complex tasks to personnel within the military organisation.

However, there is the unfortunate possibility that these protection measures may be ineffective, if there are traitors within the network that contribute to compromising the security measures of the system.

Therefore, in order to grant privileges to use the network resources, users must be ranked on several levels of trust, depending on how long they have been acting in that network, their behaviour and the severity of security events in which they were involved.

Remote attack is an action initiated on a communications network or on a network equipment, when the aggressor initially has no control.

The remote attack can be carried out in three stages:

The first stage is an information one, in which the attacker must discover information about:

- network administrator;
- network equipment and their functions;
- operating systems used;
- vulnerability points;
- network topology;
- security policies etc.

This first stage is assimilated to an attack, called a **reconnaissance attack**, and consists in the unauthorised mapping of a computer system, its services and its vulnerabilities.

The second stage is one of tapping and consists of cloning a target and attacking it, to simulate the response mode.

The third stage is to launch the attack on the network. A successful attack runs fast when the network presents vulnerabilities.

According to another classification of the attacks addressed to the communications/information networks, according to the way they are carried out, as a destination and source, the attacks can be **focused** on a single target (a particular server from a single device is attacked) or they can be **distributed** (initiated from multiple locations or by multiple equipment at the same time).

According to the way the attacker interacts with the unauthorised accessed information, as a result of the successful action, two categories of attacks are distinguished: **passive** and **active**.

Passive attacks are those attacks where the attacker only monitors the way information flows through the system without interfering in this flow. Also, in the category of passive attacks, the interception itself (radio, fibre/optic fibre) and the goniometry (radio) are included.

Passive attacks are those attacks where the attacker only monitors the way information flows through the system without interfering in this flow. Also, in the category of passive attacks, the interception itself (radio, fibre/optic fibre) and the goniometry (radio) are included.

Passive attacks may have some common characteristics:

- they do not create immediate and detectable damages, because they do not delete or modify data, do not block the network, do not disturb the traffic;
- they violate the confidentiality rules;
- the goal is to listen to the data exchanged on the communication channels;
- the listened data are subject to other processing stages, in order to extract the information useful for other operations, including other passive attacks;
- they are difficult, even impossible, to notice.

These attacks can be carried out by various methods, such as: surveillance of telephone calls, radio or radio broadcasts, exploitation of emitted electromagnetic radiation, for the purpose of transmitting information or compressive parasitic radiation, data routing, through weaker protected secondary nodes.

Active attacks are attacks through which the attacker materialises his action in the destruction, theft, alteration or resuming the messages or inserting false messages.

Active attacks are aimed at stealing or falsifying information transmitted or stored in the network, reducing network availability, by overloading it with packets (flooding), disrupting or blocking communications, by physical or logical attack on network equipment, and communication paths.

These attacks are more dangerous because they change the state of the computing, management and switching systems, as well as the data. There are a number of active attacks, in which case a new analysis is required, according to the criterion of the effect produced by them, as follows:

a. Attacks that mainly affect the organisational state:

- electronic jamming – consists in modifying the reception signals;
- disinformation – is achieved by intercepting and modifying the content of the message, followed by a timely retransmission of the communication;
- masquerade – is an attack, in which a network target (user, client, service or server) indicates another identity to retrieve confidential information (passwords, identification data, encryption keys, credit card information and other);
- replay – occurs when a message or component thereof is resumed (repeated), with the intention of producing an unauthorised effect;
- modification of messages – the message data are subjected, in an unauthorised way, to modification, insertion or deletion;
- Denial of Service attack (*DoS*) – occurs when an authorised entity fails to perform its function or when an intruder performs actions, which hinders another entity in performing other functions;
- service repudiation – occurs when an entity does not want to recognise a service performed.

b. Active attacks with a predominantly destructive effect – in the systems dependent on the computerised components, are realised by means of programs created for this purpose, which sometimes affect the computer security, including the servers. These attacks aim at unauthorised reading of information, but most often, partial or total destruction of data or even processing equipment. Of these destructive programs, we mention the following:

- viruses – represented by computer programs, which multiply by themselves in the programs of the attacked system, using the resident space in the memory/hard disk and blocking

the computer or, after a programmed number of multiplications, they can even cause damage;
- software bomb – is a part of a code or procedure, inserted in a necessary application, which can be launched by a scheduled event. The bomb maker informs about this event, letting it carry out the destructive actions programmed by the effect of the *"explosion"*;
- worms – most often produce destructive effects, similar to those of bombs and viruses. The difference is that the worms do not reside at a fixed address or multiply by themselves. Instead, they move permanently, which makes it very difficult to detect;
- The Trojan horse – is an application, which comes in the form of a known use function and which, concealed, fulfils another function.

There are many possibilities of attacking information systems, which can exploit their vulnerabilities.

Software bomb – is a part of a code or procedure, inserted in a necessary application, which can be launched by a scheduled event. The bomb maker informs about this event, letting it carry out the destructive actions programmed by the effect of the "explosion".

SPECIFIC INFORMATION SYSTEM VULNERABILITIES

Informational vulnerabilities are a component of the security vulnerability of the systems, generated by the factual states or internal processes of the organisation, which can reduce the response capabilities to possible threats, of any kind, including information.

Generally, information vulnerabilities are greater as the information networks and information structure are more complex, so they are harder to manage, being harder to organise and protect.

Also, it is considered that *"vulnerabilities increase directly proportional to the technological level implemented in the construction and operation of information systems equipment (particularly digital)"*[38].

The most known vulnerabilities, in the case of military information systems, are:
- errors in system design and operation;
- possibility of some technical components to fail;
- difficulties in the integral and integrated testing of the system;

[38] C. Alexandrescu, G. Alexandrescu, Gh. Boaru, *Sisteme informaţionale militare – servicii şi tehnologie*, Editura UNAp *"Carol I"*, Bucureşti, 2010, p. 294.

- excessive amount of information to be analysed;
- dispersion of users and access points over a wide geographical area;
- insufficient training of personnel in the national security field;
- failure to execute a new security accreditation, after a system modification;
- connecting computers from unclassified local networks to other classified networks;
- incorrectly configured/entered routers and firewall addresses;
- non-compliance with TEMPEST norms;
- exceeding the deadlines for changing passwords and encryption keys;
- non-restriction of Dal-in connections in LAN and non-restriction of electronic mail service;
- use of unclassified channels, for the transmission of classified information.

Regarding the analysis of the information infrastructure, it is considered that the main vulnerabilities could be the following[39]:
- the possibilities of intercepting information in the communications networks and computers both inside (by users) and outside (by opponents);
- the very large volume of information produced, transmitted and processed in the information systems, which can be subjected to research and attack, destroyed, forged or stolen by potential adversaries;
- the difficulty of managing the information infrastructure, due to its complexity, which determines the impossibility of detecting fraudulent access to information and favouring cyber-attacks;
- using the same frequency bands of both their own means and of potential adversaries;
- standardisation of the technical equipment, software components and databases used;

[39] C. Alexandrescu, *Ameninţări şi riscuri electronice privind sistemele informaţionale militare moderne în spaţiul de luptă*, in the volume of the Scientific Papers Session organised by *"Carol I"*, NDU – Information Systems SI-2007, pp. 107-115.

- the use of common elements of the national information infrastructure, which creates conditions for fraudulent access and disinformation;
- the possibility for the equipment supplying companies to previously incorporate, in the computing and communications equipment, some malicious software modules, which can be activated by the opponents, at certain times established by them, creating clutter and chaos in the information and in the decision-making networks;
- vulnerabilities to unauthorised intrusions (with malicious intent or lack of attention) due to the fact that organisations are connected to the Internet, Intranet or Extranet;
- failure to fully comply with EU and NATO requirements and standards regarding the compatibility and interoperability of information systems, particularly in terms of information exchange (message format), access to databases, automatic encryption of communications and the connection channels' characteristics;
- the possibility of using by potential opponents of the electronic warfare against the radio-electronic means of the main information and communication systems, especially on the channels that ensure the connection of the sources of information with the central bodies of fusion and data processing;
- the interception by the adversary (hostile forces) of the communications transmitted by radio, their decryption in a timely manner, in case of using non-performing cryptographic systems, and the use, for their own purposes, of this information, in order to obtain the information superiority;
- the current technical means of the information systems have not ensured the sound protection against the physical, electromagnetic and cyber-attack, these can be destroyed, damaged or extracted;
- placing the technical equipment (mostly the communication and computing means) of the information system in areas considered inadequate from the functional and physical/ electromagnetic security point of view, which increases

the vulnerability of interception of the information and of physical attack;
- using, for the information systems exploitation, of insufficiently verified and not loyal persons, predisposed to be recruited by potential adversaries and determined to carry out sabotage actions or to provide them with information obtained fraudulently;
- neutralising the shortwave radio link, especially at long distances, based on the propagation of electromagnetic waves, through the ionosphere, by changing its electrical characteristics;
- the existence, to the potential adversaries, of the electronic weapons with infra-acoustic radiation, based on the propagation in space of the subsonic waves, which act on the personnel, causing serious failures, vomiting, nausea, fear, depression etc., determining their inactivation, for certain periods of time, and, implicitly, the interruption of the information systems' functioning;
- installing antennas of the communication means in the open field or in spaces without natural protection properties, which allows slight malfunction and interruption of the connections, especially those made with radio stations and/or high-power radios;
- suppressing the information systems' access to the Internet, in order to isolate them and prevent the use of information from open sources;
- use of the Internet for terrorist actions, disinformation and cyber-attacks on information infrastructure;
- improper infrastructure design, with reduced information redundancy, excessively centralised and with low possibilities of existing information replication in the databases;
- insufficient concern for the concealment and masking of the information infrastructure elements, inadequate security and defence measures;
- insufficiently studied measures to ensure communications security (COMSEC), computers security (COMPUSEC) and electronic

equipment as a whole by prohibiting (restricting) parasitic radiation interception (TEMPEST – Transient Electromagnetic Pulse Emanation Standard protection).

From the analysis carried out, it turns out that there are numerous vulnerabilities, but, among these, the most important ones are those concerning: optimal organisation of information systems, improper choice of the technical equipment used and of the commercial software products, the manufacture of the application software and the databases, as well as software, for the automatic encryption of information in information systems, unfair or insufficiently verified personnel.

There are numerous vulnerabilities, but, among these, the most important ones are those concerning: optimal organisation of information systems, improper choice of the technical equipment used and of the commercial software products, the manufacture of the application software and the databases, as well as software, for the automatic encryption of information in information systems, unfair or insufficiently verified personnel.

CONCLUSIONS

In the new global information environment, technological development has brought, along with the advantages and facilities it provides, a series of threats, risks and vulnerabilities to the security of information and information systems.

Concerns about addressing threats, vulnerabilities and risks, in the specific dynamics of the last decades, include an extended area, important efforts being concentrated in the information field.

Considering that information attacks are a threat to the information systems security, specialists are trying to implement new methods of fighting against information and information attacks, which are mainly aimed at protecting their information and information systems.

Starting from the fact that there can be no absolute control, but merely a limitation, the experts have launched a new offensive, in order to improve the legislation, strengthen the role of the profile agencies and to perfect the products necessary for the detection of IT and information crimes.

For a vulnerability to be exploited, it must be known or discovered by a threat. This makes it important to follow the application of the "*need to know*" principle, while complying with security measures and their application both by personnel and in the field of technology.

This makes important the appropriate reaction of the institution, in identifying any vulnerability that may affect it.

We appreciate that estimates can be made, with a certain level of confidence, but it is difficult, scientifically, to accurately analyse threats

to information systems. These estimates depend, first and foremost, on the human factor, its mindset, its subjectivity and the implying uncertainty.

Ensuring the security of military information systems is a complex and difficult activity, as this is done through the implementation, within or outside the national territory, based on the international and coalition/national and international laws and regulations, of some specific measures which, as a rule, are: general, organisational, physical protection, personnel protection, document protection, legal and procedural protection, industrial security, as well as particular measures, computer system and communications security.

The security of the communications and information system, a component of the information system (C4I), aims at protecting information, the hardware and software components, through efficient measures, which can prevent the access to information and the interference in the information processes (collection, transmission, storage, processing, distribution, conversion, display).

In local computer networks and in the communications system, security measures must ensure: authentication (verification of the identity of a remote communication entity); control of access to resources; data confidentiality; data integrity; physical protection of technical equipment.

Generally, the security of information systems is a very complex field, in which the entire personnel is involved and which, through the restrictions and algorithms that they adopt and impose, often generates excess contradictions and bureaucracies. With all the shortcomings and drawbacks it can generate, it is better to follow the rules than to jeopardise the mission.

The increasing dependence of the command and control activities on the security of information systems leads to the increase in the typology of vulnerabilities that organisations must face.

Moreover, the issue of protection often has to consider the interconnection of private networks with public services. If we add to this aspect the problem of information sharing, a rather complicated picture is outlined, in which the implementation of effective controls becomes a difficult task for the IT&C specialist.

We consider that information security is not just a technical problem, but it is, first of all, a managerial problem.

The ISO/IEC 17799 security standard responds to the needs of organisations of any type, public or private, through a series of information security management practices. The standard can be used, depending on the degree of exposure of each organisation individually, to raise awareness, at the management level, of information security issues, or to create an organisational culture regarding information security, or to obtain information certification for the security system.

The ISO/IEC 17799 security standard responds to the needs of organisations of any type, public or private, through a series of information security management practices. The standard can be used, depending on the degree of exposure of each organisation individually, to raise awareness, at the management level, of information security issues, or to create an organisational culture regarding information security, or to obtain information certification for the security system.

Establishing the security requirements, the necessary measures to ensure the desired level of control, has a subjective component, being difficult to quantify, in monetary terms, the loss suffered, in the event of a security incident.

From the study of this very complex field of information security and military information systems we consider a few distinct measures:

- optimal organisation of information systems, so as to ensure the fundamental condition, for their efficient functioning – their reconfiguration, mobility and adaptability to the constantly developing information environment;
- keep in mind the conditions, restrictions and standards that are set, as a member of the EU and NATO. These require to be fully respected and applied firmly, in order to meet the compatibility and interoperability criteria with other organisations in the country and abroad;
- the classified information will be disseminated only to persons who hold an appropriate security certificate;
- compliance with NATO regulations[40], whereby the application of the minimum standards for ensuring the security of information is mandatory for all personnel who has access in the information system;
- increasing responsibility and control for the protection of classified information by each person who owns, processes or is aware of such information;

[40] *AD 70-1*, *ACO Security Directive*, NATO HQ, Brussels, 2006, p. I-2-4.

- periodically carrying out risk assessments on information systems and their processing in front of military personnel, in the form of lessons learned;
- purchase of new information technologies to take into account the purpose of reducing the specific vulnerabilities;
- the professional training to include topics in the field of information security and information systems.

In conclusion, in the current information age, technological security is of particular importance and also concerns the computer networks (COMPUSEC) and the communication networks (COMSEC).

Unfortunately, there is no 100% safe security system. However, by defining a realistic security policy, the most effective ways of avoiding the risks to which the military information network is subjected must always be found.

BIBLIOGRAPHY:

1. ***, AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008.
2. ***, AD 70-1, *ACO Security Directive*, NATO HQ, Brussels, 2006.
3. ***, AJP-3(C), *Allied Joint Doctrine for the Conduct of Operations,* NATO, 2019.
4. ***, AJP-2*, The Allied Doctrine for Intelligence, Counterintelligence and Security,* 2003.
5. ***, *Doctrine of the Romanian Armed Forces*, Bucureşti, 2012.
6. ***, *Doctrine of Intelligence in Joint Operations* (of the Canadian Armed Forces), 2003.
7. ***, *Doctrine for the Armed Forces Intelligence, Counterintelligence and Security*, Bucureşti, 2005.
8. ***, *Doctrine of Intelligence Support to Joint Operations,* 2003.
9. ***, FM 3-13, *Information Operations*, Washington DC, December 2016.
10. ***, FM 101-6, *Information Operations*, 1996.
11. ***, *Guidelines for the National Defence Strategy for the period 2015-2019*, Presidential Administration, București, 2015.
12. ***, IPS-3, *Doctrina pentru informații, contrainformații şi securitate a Armatei*, București, 2005.
13. ***, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 2016.
14. ***, JP-2, *Intelligence in Joint Operations* (of the US Armed Forces), 2007.
15. ***, *Law no. 182/2002 on classified information protection.*

16. ***, *Norms regarding classified information protection in the Ministry of National Defence, approved through the Order of the Minister of National Defence no.M.9/2013,* published in the Official Gazette of Romania, Part 1, no. 115, on 28 February 2013.
17. ***, *National Strategy regarding Digital Agenda for Romania 2020,* approved by Government Decision no. 245/7 April 2015.
18. ***, *Romania's National Defence Strategy: "For a Romania that guarantees future generations security and prosperity"*, București, 2010.
19. ***, *Romania's National Security Strategy*: *"European Romania, Euro-Atlantic Romania: for a better life in a democratic, safer and wealthier country"*, Bucureşti, 2007.
20. ***, *Romanian Armed Forces Transformation Strategy*, București, 2007.
21. D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington D.C., CCRP-Data publication, August 2001.
22. C. Alexandrescu, *Ameninţări şi riscuri electronice privind sistemele informaţionale militare moderne în spaţiul de luptă*, in the volume of Scientific Papers Session of *"Carol I"* NDU – *"Information Systems SI-2007"*.
23. Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale – fundamente teoretice –*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2009.
24. G. Alexandrescu, G. Boaru, C. Alexandrescu, *Sisteme informaţionale pentru management,* Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2012.
25. Francisco Martínez Álvarez, Alicia Troncoso Lora, José António Sáez Muñoz, Héctor Quintián, Emilio Corchado, *Synthesis Informational Security International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019): Seville, Spain, 13-15 May, 2019 Proceedings,* Series: Advances in Intelligent Systems and Computing 951, Springer International Publishing, 2020.
26. Colonel (ret.) Professor Dr Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, published by the Academy of Romanian Scientists, No. 2, 2018.
27. Colonel (r.) Professor Dr Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, No. 2, 2017.
28. Colonel (r.) Professor Dr Gheorghe Boaru, Colonel Iulian-Marius Iorga, *Ciclul informational ca process, procesul și ciclul "Intelligence" în cadrul acțiunilor militare moderne,* Revista de Științe Militare, published by the Academy of Romanian Scientists, No. 1, 2017.

29. Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acţiunile militare,* Editura AÎSM, Bucureşti, 2003.
30. Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informaţională şi protecţia informaţiilor*, Editura Detectiv, Bucureşti, 2006.
31. Abhishek Chopra, Mukund Chaudhary, *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines,* Apress, 2020.
32. Vasile Dumitru et al.*, Sisteme informaţionale militare*, Editura CERES, Bucureşti, 2000.
33. James Dunningan, *O nouă ameninţare mondială Cyber-Terorismul*, Editura Curtea Veche, 2010.
34. Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne,* Editura Universității Naționale de Apărare *„Carol I"*, București, 2018.
35. W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, Editura Tehnică, Bucureşti, 1970.
36. Ovidiu Nicolescu et al., *Sistemul informaţional managerial al organizaţiei*, Editura Economică, București, 2001.
37. Ramjee Prasad, Vandana Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology,* Springer Series In Wireless Technology, 2020.
38. *ENISA-Country Reports, 2008*, http://www.enisa.europa.eu.
39. *Information Systems*, Wikipedia, the free encyclopedia, http:/en.wikipedia.org/wiki/Information Systems.
40. *Information Security*, http:/en.Wikipedia.org/wiki/information security, 2009.
41. https://*fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/*.
42. www.dodccrp.org.

THE USE OF MASS MEDIA AS A HYBRID WARFARE INSTRUMENT

Captain Marian-Valentin BÎNĂ
"Carol I" National Defence University, Bucharest

Major Cristian DRAGOMIR
"Carol I" National Defence University, Bucharest

The aim of this paper is to analyse the combat system that the media employed in relation to Russian disinformation campaigns in a supposed context of hybrid warfare. The exposure of the news offered by the main media channels allows for the analysis of the concept of hybrid warfare to be concentrated and for its comparison with the traditional strategic conception, in order to determine if the activities in question can be classified in this type of conflict. Information warfare and related components such as cyber warfare, electronic warfare and more, are becoming increasingly complex and can be used both defensively and offensively in the current security context offered by the national media.

Keywords: hybrid warfare, media, propaganda, strategic ability, Russian Federation.

INTRODUCTION

The incorporation of information and communication technologies (ICT) has brought about a total change in the way we interact and communicate, but also in the way we inform ourselves. The expansion of what we know today as the Internet has allowed millions of people around the world to have access to the largest source of information in human history, primarily through smartphones, personal computers and state-of-the-art tablets.

The expansion of what we know today as the Internet has allowed millions of people around the world to have access to the largest source of information in human history, primarily through smartphones, personal computers and state-of-the-art tablets.

One of the areas where the spread of the Internet has had the greatest impact is communication, in the structure of the media, in the field of its audience and in the content itself. Traditional media has been forced to adapt its organisation to new formats and to continuous demand for information from readers, in addition to the emergence of new media, exclusively digital. But this request for information has also raised some doubts about the credibility and quality of information, which is a real concern if we consider the importance of the media in democratic societies. The speed at which news is currently being propagated – through websites, media or social networks – has an almost immediate and, in many cases, ephemeral impact on public opinion. The need to continuously generate news means that they have a huge volatility, while conditioning the quality of the information.

In this context, public complaints by Western governments regarding alleged misinformation campaigns led by the government of the Russian Federation have concentrated much of the attention of the international media. Concepts such as cyber-attacks, fake news, and hybrid threats have become global to denounce the spread of fake news in order to destabilise internal processes such as the Brexit, on 20 June 2019, the US presidential elections, and the Catalan political and social crisis from Spain, which reached its peak in October 2017.

According to the statements, attempts to intervene would be based on the use of information understood as a military element, of an asymmetrical nature, in a supposed context of hybrid warfare, directed by the Russian Federation against Western democracies, through the so-called *"Gerasimov Doctrine"*.

METHODOLOGY

The purpose of this analysis is to compare the journalistic treatment that the media has offered to disinformation campaigns and to Russian hybrid problems. The concept of *"hybrid"*, developed traditionally from a strategic-military field, influenced the events mentioned above in the current context of the hybrid warfare, as emphasised by most media and analysts in the field.

The article starts from the presentation of a series of news related to the disinformation campaigns of Russian origin and the influence that the concept of hybrid warfare had. Due to the large amount of news published on these issues, from the synthetic procedure, a general selection of news from various prestigious national and international media such as *The Guardian, The Washington Post, BBC* and the *Later Country* have provided a variety of perspectives, and following descriptive method, the term hybrid warfare is introduced, from its traditional conception, starting from the origin of the concept, exposing some general definitions and characteristics and contextualising it in what has become popular as Gerasimov doctrine. Finally, by comparative method, the journalistic treatment of this type of conflict is compared with the traditional strategic conception.

CONTEXTUALISATION OF HYBRID WARFARE

In recent years, taking as a temporary reference the referendum that took place in the UK to leave the European Union and especially after the US presidential elections held in November 2016, the media has concentrated much of its international information, warning of the danger posed by hoaxes – popularised as fake news – for Western democracies.

With the purpose of informing, the media has used all kinds of concepts, new to a large part of the public, such as cyberspace, cyberattack, cyber warfare or hybrid warfare, to explain the events that occur through what we commonly call the Internet, in which a state, in this case the Russian Federation, would use the digital sphere to interfere with another's internal processes, in order to destabilise its democratic systems. In this unique and complex context, here's how the media reported on events.

Although Brexit is now considered an example of Russian interference in the election campaign[1], we have found few references in the media that, both during the campaign and in the post-referendum period, accused the government of Vladimir Putin of wanting to influence the vote, defining such activities as hybrid warfare. Most of post-election analyses focused on the uncertainty generated by the United Kingdom's exit from the European Union, the economic, political and social consequences that could follow, as well as the new role of the European Union at that time.

To a large extent, it was only in the US presidential elections, held in November 2016, that the media directly indicated Moscow to have carried out computer attacks against the Democratic Party and orchestrated misinformation campaigns to influence voting through public opinion. At that point, the emphasis was placed on cyberspace and the vulnerabilities it represented for Western democracies. Despite it, only after a few months began to appear continuously information about the possible Kremlin interference in the British referendum, through the spread of fake news, as well as through the use of social media.

The events marked, before and after, the role that a foreign power would have played in trying to influence an internal electoral process. It was a warning signal for the European countries, as they were going to organise different electoral processes during the following months.

With the purpose of informing, the media has used all kinds of concepts, new to a large part of the public, such as cyberspace, cyberattack, cyber warfare or hybrid warfare, to explain the events that occur through what we commonly call the Internet, in which a state, in this case the Russian Federation, would use the digital sphere to interfere with another's internal processes, in order to destabilise its democratic systems.

[1] The Cipher Brief, The Use of Disinformation in the British Election, https://www.thecipherbrief.com/column/soufan-center/the-use-of-disinformation-in-the-british-election, accesat la data de 20.02.2020.

In this context, the Guardian newspaper stated in a headline that *"the EU is intensifying its campaign against Russian propaganda"*[2] because of the fear that would have generated the possible Russian influence in the US elections, as it could extend to Europe. It is emphasised that the Union will *"step up efforts to counter Russia's hybrid war campaign after Donald Trump's election"*[3]. The news refers to the *East StratCom Task Force*, an organisation created in 2015 – and therefore before the processes presented here – by the *EU External Action Service* to counter Russian misinformation campaigns during the crisis in Ukraine.

In this international context of misinformation, fake news, Russian influences in electoral processes, cyberattacks and alleged hybrid warfare, Spain was plunged into a major political and social crisis because of a referendum by the regional government of the *Generalitat de Catalunya*, at the beginning of October 2017, which was intended to decide by consultation on the possibility of independence from the Spanish state, without the consent of the Spanish government. Those activities were quickly incorporated into the information language. Titles such as *"Cyberwar between the Catalan and Spanish Governments to Close the Referendum Site"*[4], published in the *El País* newspaper a few days before the referendum or *"The Great Catalan Cyberwar of 2017"*[5], published by *The Washington Post*, just two weeks after the referendum was held, used the concept of cyberwar in a generic way, regardless of its significance and possible implications, for the simple fact that certain activities were carried out through the network.

The concept of cyberwar has been one of the most used in the journalistic field to refer to the activities that take place on the Internet,

[2] Daniel Boffey, Jennifer Rankin, *"EU Escalates Its Campaign against Russian Propaganda"*, The Guardian, 5 December 2018.

[3] Daniel Boffey, *"EU Raises Funds to Fight <Disinformation War> with Russia"*, The Guardian, 5 December 2018.

[4] Jordi Pueyo, *"Ciberguerra entre los gobiernos catalán y español por el cierre de la web del referendum"*, El Pais, 14 September 2017, https://elpais.com/ccaa/2017/09/14/catalunya/1505390726_024743.html, retrieved on 04.08.2019.

[5] Christian Caryl, *"The Great Catalonian Cyberwar of 2017"*, The Washington Post, 18 October 2017, https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fnews%2fdemocracy-post%2fwp%2f2017%2f10%2f18%2fthe-great-catalonian-cyberwar-of-2017%2f, retrieved on 04.08.2019.

but in its turn, it has created confusion. Richard A. Clarke, former US National Security, Infrastructure Protection and Counter-Terrorism Coordinator and President's Special Adviser on Cyber Security, defines cyberwar as *"actions taken by a nation-state to break into other state computers or networks for the purpose of causing damage or alteration"*[6]. Except for the cyberattacks against the Democratic Party, for which he had access to the campaign data and information of the Party members, the propaganda activities that took place in Brexit and in the Catalan conflict cannot be described as cyberwar, according to Clarke's definition, as they would not have led to the illegitimate access to the systems or networks of other states, in order to cause damages or changes, but rather they would be influential and manipulative activities through the network.

This new doctrine, developed in Russia, seeks to weaken democracies, mixing in their electoral processes and fuelling their internal conflicts, whether ideological or territorial, using tools such as fake news or manipulation of social networks.

Instead, it is said that we are in a conflict (hybrid war) promoted by a state actor (Russia), by spreading fake news over the Internet and social networks, with the ultimate goal of weakening Western democratic governments. On the other hand, the pieces of news on these activities present the hybrid war as something new, which is part of a military doctrine of Russian origin known as the Gerasimov doctrine.

THE ORIGIN AND CHARACTERISTICS OF HYBRID WARFARE

There are authors who attribute the origin of the term hybrid warfare to the retired US Marine General Robert Walker, who, in 1998, analysed the hybrid model of wars in a paper. On the other hand, there are those who point out that the origin should be placed a few years later, in 2002, when the term was used to explain the tactical actions

There are authors who attribute the origin of the term hybrid warfare to the retired US Marine General Robert Walker, who, in 1998, analysed the hybrid model of wars in a paper. On the other hand, there are those who point out that the origin should be placed a few years later, in 2002, when the term was used to explain the tactical actions of the First Chechen War, which took place between 1994 and 1996.

[6] Richard A. Clarke, Robert K. Knake, *Cyber War, the Next Threat to National Security and What to Do about It*, EEUU, Harper Collins Publishers, 2010.

of the First Chechen War, which took place between 1994 and 1996. However, they were not officially used until the 2005 US National Defence Strategy[7]. It was only in 2005, when General James N. Mattis and Colonel Frank G. Hoffman published the article *Future Warfare, the Rise of Hybrid Warfare*, and Frank G. Hoffman published the *Conflict in the 21st Century, the Rise of Hybrid Warfare*, that the concept gained theoretical content and became popular.

The concept has been largely extended to try to understand contemporary wars between state and non-state actors, in which a top theoretical actor in the field of technology, military or doctrinal capacity could be surprised by a non-state actor.

Definitions of Hybrid Warfare

The hybrid war is "one in which at least one of the opponents uses a combination of conventional operations and irregular war, mixed with the latter, with terrorist actions and connections to organised crime".

One of the first approaches defines hybrid warfare as *"the one at the intersections between special war and conventional war"*[8]. On his part, Hoffman broadens and specifies its nature and considers that *"it mixes the lethality of the state conflict with the fanatical and widespread fervour of the irregular warfare"*[9]. It can be promoted by both state and non-state actors. These conflicts *"incorporate a variety of different ways of conducting war, including conventional capabilities, irregular tactics and formations, terrorist activities, including violence and coercion without discrimination and criminal disturbance"*[10]. In practice, this involves the combination of conventional and irregular activities. In a similar vein, the Infantry Colonel of the Spanish army, José Luis Calvo Albero, defines the hybrid war as *"one in which at least one of the opponents uses a combination of conventional operations and irregular war, mixed with the latter, with terrorist actions and connections to organised crime"*[11].

[7] Guillem Colom, *"La amenaza hibrida: mitos, legendas y realidades"*, Instituto Espanol de Estudios Estrategicos, Documento de Trabajo, http://www.ieee.es/contenido/noticias/2019/03/DIEEEO24_2019GUICOL-hibrida.html, retrieved on 19.01.2020.

[8] Robert G. Walker, *"Spec Fi, the United States Marine Corps and Special Operations"*, Naval Postgraduate School, https://archive.org/details/specfiunitedstat00walk/mode/2up, retrieved on 09.02.2020.

[9] Frank G. Hoffman, *Conflict in the 21st Century, The Rise of Hybrid Wars*, Institute for Policy Studies, Potomac, Virginia, 2007.

[10] *Ibidem.*

[11] Jose Miguel Palacios, *"Rusia: guerra hibrida y conflictos asimetricos"*, Ejercito, 904, July-August, 2016, pp. 22-27.

Despite these approaches, there is currently no precise definition of the concept, which is widely accepted, beyond the smallest common denominator of the combination of conventional, asymmetrical means, procedures and tactics. In post-Cold War conflicts, those who faced Western states would, at times, have used conventional forces, irregular troops, terrorist acts and organised crime.

Characteristics of Hybrid Wars

The news has presented the hybrid war as a unique conflict, focusing mainly on the information element, misinformation and fake news, and its dissemination on the Internet. But such conflicts would also involve the combination of other elements to consider, such as the actors involved, the type of weapons they have and the scenarios that are constantly developing. Some features of hybrid wars are:

❖ *The physiognomy of the actors involved*: these include states, guerrilla groups and terrorists, as well as organised crime groups or private military contractors. These types of conflicts can be assumed by state actors or non-state actors. As noted above, the analyses of hybrid warfare have focused mainly on the confrontations between non-state actors, regularly attacked by a failed state, and Western states, such as in the wars in Afghanistan, Iraq, and the confrontation between Hezbollah and Israel. Insurgent groups would develop hybrid warfare because they would have lower capabilities than state actors, and deficiencies in personnel, doctrine, weapons and technology. Comprising mainly volunteers, the aim would be to counteract the superiority of the state actor and exploit its vulnerabilities. On the other hand, this type of conflict can also arise from the state actors, in a possible conventional confrontation with other state actors, superior from a military point of view. An unusual case would be the conflict between Ukraine and Russia in 2014, in which the most theoretically powerful state, Russia, was the one that used the hybrid war against the least developed one. This decision would be based on avoiding a conventional confrontation and, in turn, on a possible confrontation

The analyses of hybrid warfare have focused mainly on the confrontations between non-state actors, regularly attacked by a failed state, and Western states, such as in the wars in Afghanistan, Iraq, and the confrontation between Hezbollah and Israel.

with the United States and NATO, in which Russia would be the affected party.

❖ *Type of weapons used*: Irregular forces have more armament than ordinary armies, such as the latest technologies and heavy weapons, which makes it more difficult to distinguish between conventional and irregular forms of war.

❖ *The tactics used*: from the use of conventional actions to terrorist acts, the use of insurgent actions, informative operations or computer operations.

❖ *Use of information and communication technologies*: this feature of hybrid warfare includes the control of traditional media up to the Internet and social networks. This would make it possible to strengthen one's own image or to counteract that of the adversary, in order to reach the *"hearts and minds of people"*[12], which would be largely psychological warfare. In this way, there is an increasing importance of the so-called information warfare and the use of cyberspace.

Irregular forces have more armament than ordinary armies, such as the latest technologies and heavy weapons, which makes it more difficult to distinguish between conventional and irregular forms of war.

❖ *Scenarios for the battle space*: these types of conflicts are considered essentially urban, as opposed to guerrilla wars, which would take place in the jungle or mountains. This aspect creates greater difficulties in achieving the military objectives, due to the presence of the civilian population and the possible consequences on the critical infrastructure, such as transport and energy.

❖ *Liaison with terrorist groups and organised crime*: It is common for groups involved in hybrid wars to have links with terrorist groups or organised crime. This does not necessarily imply that they have common goals.

❖ *The increasing importance of the psychological element*: there is an intentional disregard for the legality and international humanitarian law by the promoters of hybrid wars and the related criminal and terrorist groups. On the contrary, the Western armed

[12] James K. Wither, *"Making Sense of Hybrid Warfare"*, Connections, the Quarterly Journal 2, 2016.

forces are subject to rules, military traditions or confrontation rules. Therefore, hybrid wars can be considered formally different from traditional conflicts, in that they "*have been fought conventionally and symmetrically on clearly defined fronts, with time-advanced technological means and subject to the commonly accepted uses and customs of war for competitors"*[13].

❖ *Planning*: the promoters of this type of conflict would have previously detected the weaknesses of the adversary, in the political, ideological, economic or demographic field, in order to prolong the conflict, to increase the costs or to influence the perception of the societies and of the Western states.

It should be noted that hybrid wars involve the combination of regular and irregular elements. Therefore, the use of one of these elements does not imply that a conflict can necessarily be considered *"hybrid"*. Russian activities in the cases – Brexit, the US elections and the Catalan conflict, have received the hybrid qualification largely due to the use of cyberspace and the combination of computer attacks, propaganda and misinformation, the use of information and communication technologies, as well as information operations. However, it was by no means an armed confrontation involving state or non-state actors.

ROMANIAN MILITARY THINKING

Hybrid wars involve the combination of regular and irregular elements. Therefore, the use of one of these elements does not imply that a conflict can necessarily be considered "hybrid". Russian activities in the cases – Brexit, the US elections and the Catalan conflict, have received the hybrid qualification largely due to the use of cyberspace and the combination of computer attacks, propaganda and misinformation, the use of information and communication technologies, as well as information operations.

HYBRID WARFARE AND THE RELATIONSHIP WITH THE MASS MEDIA

According to the press, Russia is waging a hybrid war against Western states. However, the above classification presents a different scenario from those described. The novelty, according to the news, is that only one state, Russia would wage such wars simultaneously against several states, including the main military powers such as the United States of America and the United Kingdom. This, through a continuous process that extends over time, but in which we can identify high pressure moments, for example, shortly before the electoral

[13] Guillem Colom, *"La Doctrina Gerasimov y el pensamiento estrategico ruso contemporaneo"*, Ejercito, 933, December, 2018.

processes in the UK. Despite the development that Russia has made in the digital sphere, along with misinformation campaigns, it has no monopoly on these activities[14]. However, the media has reported that it is an almost exclusive activity of Russia. It should be borne in mind that one of the fundamental characteristics of the hybrid war would be not only the use of information and communication technologies, but also the simultaneous use of other components mentioned above. That is, the combination of the usual and irregular elements referred to by Hoffman. In the supposed hybrid war between Russia and the Western states, there is no armed conflict in which regular and irregular forces participate, advanced weapons are used or terrorist acts are carried out.

One of the characteristic elements of hybrid wars is the space in which they develop, mainly urban centres. If we look at the conflict in Eastern Europe, Russia would have used cyberspace as the main stage of its activities.

One of the features emphasised by the media was the novelty of this type of conflict and the exclusivity that Russia has had in approaching hybrid wars. Some experts believe that *"these forms of action can hardly be described as new or considered as a specific response to the westernised fighting style"*[15].

On the other hand, one of the characteristic elements of hybrid wars is the space in which they develop, mainly urban centres. If we look at the conflict in Eastern Europe, Russia would have used cyberspace as the main stage of its activities. For all these reasons, although computer operations were carried out via the Internet, not only the dissemination of news, but also computer attacks such as those against the United States Democratic Party, which allowed access to email accounts, the activities were defined as hybrid war, within the events exposed to the news.

[14] The Cipher Brief, The Use of Disinformation in the British Election, https://www.thecipherbrief.com/column/soufan-center/the-use-of-disinformation-in-the-british-election, accesat la data de 20.02.2020.

[15] Guillem Colom, *"Vigencia y limitaciones de la guerra hibrida"*, Cientifica General Jose Maria Cordova, no. 1, 2012.

GERASIMOV DOCTRINE AND THE HYBRID WARFARE

If the concept of hybrid warfare was concentrated in one part of the analysis, other concepts were used to contextualise such conflicts. The media emphasised that the hybrid war was part of a Russian military doctrine that became popular as the Gerasimov doctrine, which would expose the line separating the war from peace is now widespread, so they must develop tactics to allow it, working in the shadows, conditioning the electoral processes, agitating the civilian population or hacking targets in other countries.

The origin of the concept dates from February 2013, with the publication of the article *"The Value of Science in Anticipation"* of the Chief of the Defence Staff of the Russian Armed Forces, General Valeri Gerasimov, in the journal *Voyenno-Promyshlennyy Kuryer*. For most Western media and analysts, the article is the cornerstone of what is known in the West as the Gerasimov doctrine. *"It is interpreted as a proposal for a new Russian mode of war that combines conventional and unconventional warfare with aspects of national power"*[16], which refers to indirect and asymmetrical methods. With the events in Crimea and Ukraine, some of the elements set out in Gerasimov's 2013 document have been identified and the idea that it exposes a new way of acting has been propagated.

The origin of the concept dates from February 2013, with the publication of the article "The Value of Science in Anticipation" of the Chief of the Defence Staff of the Russian Armed Forces, General Valeri Gerasimov, in the journal Voyenno-Promyshlennyy Kuryer. For most Western media and analysts, the article is the cornerstone of what is known in the West as the "Gerasimov doctrine".

The hybrid then crossed the border of strategic debate to become a word of common use, defining the full range of informational, destabilising and subversive activities that the Kremlin could conduct in a hidden, semi-covert or clandestine manner, below the threshold of conflict.

Despite the widespread acceptance of the concept and the fact that it represents a new doctrine, some analysts have questioned whether it is military doctrine or it suggests a new Russian way of waging war. It is noteworthy that Gerasimov stated in his article *"his perspective on the recent past, present and future of the war"*[17],

[16] Charles K. Bartles,*"Cómo comprender el artículo de Gerasimov"*, Military Review, 2016.

[17] Valeri Gerasimov, *"Ценностьнаукивпредвидении"*, VPK 476 8, March, 2013, https://vpk-news.ru/articles/14632, retrieved on 02.02.2020.

based largely on what happened in the *"Arab Spring"* and the *"colour revolutions"*[18]. Gerasimov emphasises non-military means, such as political, economic, humanitarian, undercover operations, as well as the importance of information. Russia, for its part, considers hybrid warfare to be a Western term and therefore different from its doctrinal system. In fact, the Russian Federation refers to different terms related to hybrid warfare, such as *"non-linear warfare"*, *"ambiguous warfare"* and *"network warfare"*[19].

Three years later, Gerasimov published a new article in which he presented some ideas about contemporary wars, apparently similar to the previous document, but in which he added the experiences of conflicts in Ukraine and Syria. Gerasimov identifies hybrid methods in colour revolutions, stating that these movements are, in fact, matters promoted by the West. Unlike the 2013 article, this document refers openly to wars and hybrid methods, but in a different way from the West.

In Gerasimov's view, in contemporary conflicts, it is increasingly common to give priority to common uses of non-military, political, economic, informational and other measures that are implemented with the support of military force.

As mentioned above, hybrid warfare would combine conventional and irregular methods, in which we found links with organised crime or terrorist groups, while, in Gerasimov's view, in contemporary conflicts, it is increasingly common to give priority to common uses of non-military, political, economic, informational and other measures that are implemented with the support of military force[20]. All of these elements integrated under the same umbrella are called hybrid methods.

In practice, this would imply a more limited perception of hybrid actions than the West. Despite this difference, the author argues that the integration of traditional and hybrid activities is a feature of contemporary armed conflicts, in which he indicates the informative

[18] *Arab Spring* was a series of anti-government protests, uprisings, and armed rebellions that spread across much of the Arab world in the early 2010s. It began in response to oppressive regimes and a low standard of living, https://en.wikipedia.org/wiki/Arab_Spring, retrieved on 24.02.2020. *Colour revolutions* is the non-violent overthrow of power by street protests, https://ro.odkurzacze.info/2746-the-most-famous-color-revolutions.html, retrieved on 23.02.2020.

[19] Mira Milosevich, *"El poder de la in-fluencia rusa: la desinformación"*. Real Instituto Elcano, ARI 7/2017.

[20] Valeri Gerasimov, *"По опыту Сирии"*, VPK 624 9, March, 2016, https://www.vpk-news.ru/articles/48913, retrieved on 23.02.2020.

element as the main of the hybrid methods. This is because the falsification of events, the limitation of the media activity, becomes one of the most efficient asymmetrical methods for carrying out wars. Its effect can be comparable to the results of the use of massive troops.

In short, Gerasimov refers to hybrid warfare methods, as he believes that Russia should cope with these types of wars and, therefore, must know and adapt to them. In addition, it must be taken into account that Gerasimov presents it in a scenario of armed warfare, while misinformation campaigns and fake news in the West would take place in a context of political and social tension and confrontation, but in the absence of an armed conflict. Last but not least, Mark Galeotti, the analyst who coined the term Gerasimov's doctrine[21], not only denied the existence of that alleged doctrine, but also noted that Gerasimov's article was intended to resolve how to combat unconventional actions.

CONCLUSIONS

It is common to find news related to misinformation campaigns of Russian origin claiming to be registered in a context of hybrid warfare against the West. The main problem with the journalistic information presented here is that, for the most part, the authors do not expose even a brief approximation to the concepts used, their meaning and implications, such as misinformation, fake news, cyberwar or hybrid warfare. Sometimes this leads to the use of some of these concepts as synonyms. Possibly, one of the reasons for the confusion is the mix between the use of recent concepts, in this case, those related to the cyber space, with others that are traditionally located in a military and academic field, in an attempt to wish to be informed about changes that appear on the international stage. This is also due to the spiral in which the media has entered, driven by a constant demand for information from citizens, wanting to inform almost minute by minute about the latest news, which means information quantity rather than the quality of the messages transmitted.

[21] Mark Galeotti, *"I'm Sorry for Creating the <Gerasimov Doctrine>"*, Foreign Policy, March, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doc-trine/, retrieved on 23.02.2020.

Undoubtedly, the use of cyber and information by Russia has been the focus of the news regarding hybrid warfare. But while it is true that this country has encouraged the use of information operations and has taken advantage of the potential of the digital environment in its interests, it is true that the development of misinformation campaigns and the use of information and communication technologies cannot be identified solely with the hybrid warfare. One of the characteristics of hybrid conflicts is the combination of different conventional and asymmetrical elements, but the news focused almost exclusively on the digital element, through which the campaigns of misinformation, fake news and the massive use of social networks were developed. Although they can be part of hybrid conflicts, and the fact that in recent years the cyber element has gained enormous importance in conflicts, we cannot stress that these activities are movements of the hybrid war.

The use of cyber and information by Russia has been the focus of the news regarding hybrid warfare. But while it is true that this country has encouraged the use of information operations and has taken advantage of the potential of the digital environment in its interests, it is true that the development of misinformation campaigns and the use of information and communication technologies cannot be identified solely with the hybrid warfare.

Therefore, if we conclude that the events that took place on the occasion of Brexit, in the US elections and in the Catalan conflict cannot be described as a hybrid war, a significant analysis framework to understand the news of cyberspace and its impact on international relations in these scenarios could be developed from the grey area concept. The concept defines those activities that are below the conflict threshold, which are conducted in peacetime, as opposed to hybrid warfare, and which include computer attacks or misinformation and propaganda campaigns that would have as a common feature the difficulty of determining their attribution. Therefore, this concept would allow an analysis of activities that are not specifically described as war actions, but could become just as decisive as a military conflict.

The analysis presented in the article focused on the importance of conceptualising and contextualising the reported facts. It is clear that the practice of journalism differs from the academic field, but it is true that the news should transmit as rigorously as possible messages and expose to the reader what is happening in a specific context, trying to use appropriate concepts in each case. We are still in an early stage in the analysis of cyberspace capabilities, and its reduction only to the

use that a single state can make for the dissemination of propaganda campaigns would mean we do not understand its potential in international relations.

BIBLIOGRAPHY

1. ***, BBC, "*Brexit: What Is Happening Now?"*, 29 June 2016, https://www.bbc.com/news/uk-politics-eu-referendum-36420148.
2. Karla Adam, William Booth, "*Rising Alarm in the UK against Russian Revenge in the Brexit Vote",* The Washington Post, 17 November 2017.
3. Charles K. Bartles, *"How to Understand Gerasimov's Article"*, Military Magazine, March-April, 2016.
4. Josep Baqués, *"Russia's Role in the Ukraine Conflict: The Hybrid War of the Great Powers"*, Journal of International Security Studies, 2015.
5. Daniel Boffey, *"EU Raises Funds to Fight <War of Misinformation> with Russia"*, The Guardian, 5 December 2018.
6. Richard A. Clarke, Robert K. Knake, *The Cyber War: The Next Threat to National Security and What Needs to Be Done*, USA, Harper Collins Publishers, 2010.
7. Valeri Gerasimov, *"Ценность науки в предвидении"*, VPK 476, 8 March 2013, https://vpk-news.ru/articles/14632.
8. Valeri Gerasimov, *"По опыту Сирии"*, VPK 624, 9 March 2016, https://vpk-news.ru/articles/29579.
9. Frank G. Hoffman, *The Conflict in the 21st Century. Rise of Hybrid Wars*, Institute for Political Studies, Potomac, Virginia.
10. Robert G. Walker, *"United States Marine Corps in Special Operations"* Master's thesis, Naval Postgraduate School, Monterey, https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf.

THE DISINFORMATION CAMPAIGNS – IMPORTANT COMPONENTS OF HYBRID WARFARE –

Captain Beng PdD Student Viorica Ionela TRINCU

"Carol I" National Defense University, Bucharest

The evolution of the international security environment and information technology has given a special impetus to the development of interpersonal and inter-community communication, especially through new media. Hybrid warfare is the most eloquent example of adapting the phenomenon of war to the evolution of human society and information technology. Disinformation has a very important role in the development and establishment of the outcome of the hybrid confrontation, which is used in all kinds of inter-community confrontation. Mass media, especially the online social platforms, are the most used and effective vehicles for carrying out and spreading disinformation.

Keywords: hybrid warfare, military stratagem, disinformation, military surprise, mass media.

INTRODUCTION

The democratic societies were based on the free expression of the citizens' will – a right that is ensured by the powers and institutions of the state under the permanent monitoring of a free and independent mass media.

The media contributes substantially to the communication between the powers and institutions of the state, on the one hand, and the population, on the other. In other words, the media collects information that is relevant to the population and makes it available to citizens in order to help them form their own opinions about the functioning of state institutions (quality of the government, transparency and accountability[1]) and the situation of the human community they belong to. Through the way it works, the mass media – monitoring and analysing the activity of state institutions – it contributes to the promotion of democracy, and through the correct information of the population, it contributes to ensuring its right to inform and to ensure free expression.

Although the media should be objective, impartial and independent[2], it has a dual role[3]. In most cases, the media in democratic states respect their self-assumed status through the codes of ethics of journalists and other media professionals, contributing to the proper functioning of democracy.

The media contributes substantially to the communication between the powers and institutions of the state, on the one hand, and the population, on the other. In other words, the media collects information that is relevant to the population and makes it available to citizens in order to help them form their own opinions about the functioning of state institutions (quality of the government, transparency and accountability) and the situation of the human community they belong to.

[1] Irina Moroianu Zlătescu, *Drepturile omului – un sistem în evoluție*, Institutul Român pentru Drepturile Omului, București, 2017, p. 3, available on http://irdo.ro/irdo/pdf/175_ro.pdf, retrieved in October 2019.

[2] Silvia Șpac, *Impactul mass-media asupra formării personalității elevului de vârstă școlară mica*, Studia Universitatis Moldaviae, 2015, available on http://ojs.studiamsu.eu/index.php/education/article/view/279/237, retrieved in October 2019.

[3] Because of the dual effects of the media, Paul Dobrescu likened communication to a despot, because this is *"a weapon, perhaps the most powerful, of conditioning and mystifying the human being"*. (*Un despot modern – opinia publică*, in *Revista română de comunicare și relații publice* no. 2-3/2000, p. 15).

In the democratic states there is partisan mass media, but also mass media belonging to some owners who obliged it to represent their interests through the audio and video articles and reports.

The media play a negative role when the intention and interest of a person (group of people) that does not agree with the general interest of the community appears. In these cases, means of influence are used, mainly disinformation and manipulation, to determine the citizens to support this interest or not to oppose the objectives of the initiator of disinformation.

Disinformation has been used successfully in all confrontations over time. Currently, this method of influencing the population has a very important contribution to the development and establishment of the outcome of the hybrid warfare.

The human losses due to the armed confrontations have caused many thinkers to initiate projects to eliminate the wars between states, respectively between communities within the states.

THE HYBRID WARFARE – A NEW STAGE OF EVOLUTION OF THE INTER-COMMUNITY CONFRONTATIONS

War has long been considered a form of armed confrontation to which political, diplomatic, economic, financial, cultural and informational actions have been associated.

About war, as a form of dispute settlement between human communities, many historical studies, literary works and articles in mass media have been written. Memorable sequences from different wars have been the main subjects of many artistic productions – films, paintings, sculptures, etc., through which deeds of heroism have been glorified or abominable actions and attitudes of some of people who had nothing in common with humanity. Their actions have been made known to the public (mass murder, terrorist attacks, destruction). deliberations of historical vestiges and places of worship, etc.).

As time has passed, mankind has experienced, including in real time in recent decades, the atrocities generated by some of the participants in violent inter-community confrontations.

The human losses due to the armed confrontations have caused many thinkers to initiate projects to eliminate the wars between states, respectively between communities within the states. Some of the most well-known projects of this kind belong to the Abbot of Saint Pierre and to Immanuel Kant. Ideas about eliminating wars

from international relations were issued by Jean Jacques Rousseau and other Renaissance thinkers. Those ideas have proven to be largely utopian because it seems that we humans have a natural tendency to confrontation[4].

The two world wars have mourned tens, perhaps even hundreds of millions of families around the world, and their conclusions have relaunched some of the ideas launched by Kant, the Abbot of Saint Pierre and other thinkers who spoke out against armed confrontation as a way of dissensions between states. As a result, some international governmental organizations have been established. They have responsibilities in the field of global (UN)[5] and regional security (Organization for Security and Cooperation in Europe – OSCE, Organization of American States – OSA, Organization of African Unity – OAU), Arab League – LA)[6] etc. They have also been drafted and ratified by most of the countries of the treated world, conventions and agreements for the prohibition of chemical weapons and anti-personnel mines, non-proliferation of weapons of mass destruction, limitation and reduction of nuclear weapons, reduction of conventional weapons in Europe, disarmament and military disarmament, etc.

ROMANIAN MILITARY THINKING

The two world wars have mourned tens, perhaps even hundreds of millions of families around the world, and their conclusions have relaunched some of the ideas launched by Kant, the Abbot of Saint Pierre and other thinkers who spoke out against armed confrontation as a way of dissensions between states.

Despite these organisational measures and the international normative acts that regulate the relations between states, respectively between citizens and their states, the violent confrontations continued in large numbers, but with a smaller number of human victims. This tendency, against the background of the end of the Cold War, determined some politico-military analysts and experts in international security to estimate that we are witnessing the decline of the war. Other reputable authors have launched predictions

[4] Majid Khadduri, *War and Peace in the Law of Islam*, John Hopkins University Press, Baltimore, 1955, p. 57, *apud* Dr. Lewis B. Ware, *An Islamic Concept of Conflict in Its Historical Context*, Blank, Stephen J, Grinter, Lawrence E., Magyar, Karl P., and Wheaters, Bynum E., *Conflict, Culture and History*, Air University Press, Maxwell Air Force Base, Alabama, USA, 1993, p. 67 *("human nature makes war a norm, not an exception").*

[5] Madeleine Albright, *Who Broke the UN*?, in *Foreign Policy*, 13.08.2012, http://foreignpolicy.com/2012/08/13/who-broke-the-u-n/, retrieved in December 2019.

[6] Roberta Cohen, *The Role of Regional Organizations*, ECOWAS, Brookings, Monday, 30 September 2002, https://www.brookings.edu/on-the-record/the-role-of-regional-organizations-ecowas/, retrieved on December 2019.

such as *"the end of geography"* (Virilio Paul - 1997)[7], *"the end of nature"* (Charles McKibben - 1990), *"the end of history"* (Francis Fukuyama – 1992), "the end of science" (John Horgan – 2012)[8] etc.

The phenomenon of war in the last century was manifested mainly by the brutal confrontation, in which the means used were mostly destructive and lethal. Currently, non-military means have the most important role in the confrontation, and the military force is kept in reserve, with the role of warning-threat, which could be used when needed, according to the principle *"when diplomacy is silent, weapons speak"*.

The phenomenon of war in the last century was manifested mainly by the brutal confrontation, in which the means used were mostly destructive and lethal. Currently, non-military means have the most important role in the confrontation, and the military force is kept in reserve, with the role of warning-threat, which could be used when needed, according to the principle "when diplomacy is silent, weapons speak".

Today, the present confrontations have mainly taken the form of hybrid warfare – a combination of concepts that us conventional and unconventional means of combat and weapon systems, designed to surprise the opponent and bring victory to the initiator.

Some authors consider that hybrid war would have appeared in the 21st century, but a brief recourse to the history of armed confrontations, only from the 20th century, reveals the existence of many similarities with the concept of hybrid warfare. There are, of course, quite a few differences because the technology has evolved a lot, both for the production of lethal and destructive means, and for those in the *"soft power"* category. It is worth mentioning the role of the international community and international governmental organisations which, through decisions and regulations, have sought to resolve differences between states peacefully, and in the event of violent conflicts to reduce the number of victims and destruction. These requirements have materialised in conceptual and technological adaptations that have reduced collateral and unnecessary losses. This is how surgical precision strikes, intelligent weapon systems, unmanned aerial vehicles, drones, research robots, military satellites, etc. were made.

The hybrid war is an example of adapting the war phenomenon to the evolution of the international security situation and the information

[7] Paul Virilio, *Un monde surexpose: fin de l'histoire ou fin de la geographie?,* in *Le monde diplomatique*, August 1997, p. 17, apud Zygmunt Bauman, *Globalizarea şi efectele ei sociale*, Editura Antet, Oradea, ISBN 973-9241-91-3, pp. 16-17.

[8] Cristopher Goker, *Future War*, Polity Press, 2014, UK, p. 137.

technology, by applying the principles of armed struggle to this situation, especially the principle of achieving surprise and avoiding surprise. Each and every military commander knows that he or she will have a better chance of winning a confrontation if he or she manages to capture the enemy. Therefore, the production of new means of combat and new weapon systems will also require an adaptation of the concepts. Under the conditions when these elements of novelty are not known by the adversaries, they constitute prerequisites for achieving surprise in the armed confrontations. Through the concept of hybrid warfare many of the conditions presented above are fulfilled, which has led some authors to assert that the war is similar to a chameleon[9], because it always changes its form and it is continuous[10].

BRIEF HISTORY OF THE USE OF DISINFORMATION IN ARMED CONFRONTATIONS

Communication is a way in which people relate to each other, but also communities, and it is a method of communication through which people and human communities intend to reach their goals, regardless of the legal and moral norms that govern human societies.

When approaching the subject of disinformation, renowned specialists from all over the world have quite different opinions, but these opinions have at least two elements in common: the interest and intention of disinformation initiators to hide (distort, truncate, modify) the reality by: inventing bomb news, minimising important events, exacerbating the importance of events that are insignificant for the public interest, etc., events and actions meant to divert public attention from the compromising aspects for the disinformation initiators or to impose ideas, projects, objectives that satisfy the interests of the initiators. The ways to achieve these goals are different

When approaching the subject of disinformation, renowned specialists from all over the world have quite different opinions, but these opinions have at least two elements in common: the interest and intention of disinformation initiators to hide (distort, truncate, modify) the reality.

[9] Mihail Orzeaţă, *Suntem pregătiţi pentru războiul viitorului?,* in *Gândirea Militară Românească* Journal no. 4 (October-December) 2016, pp. 20-29, published by Statul Major General, Bucureşti, http://www.smg.gmr.ro/gmr/Arhiva_pdf/2016/revista_4_final.pdf, retrieved in December 2019.

[10] Mihail Orzeaţă, *Războiul continuu*, Editura Militară, Bucureşti, 2011, see also Tom Toles, *Friday Rant: Perpetual War Edition*, in *The Washington Post*, 26 September 2014, http://www.washingtonpost.com/news/opinions/wp/2014/09/26/friday-rant-perpetual-war-edition/, retrieved in October 2019.

both by the means and by the methods that are used. Since Sun Tzu, considered by some to be a *"prophet of disinformation"*[11], many civilian and military experts have studied disinformation and presented their ideas in studies and papers considered to be benchmarks in the field, although some of them seem to contains *"an amalgam of terms"*[12]. To support this assertion, we present the opinions of some well-known specialists:

- *"disinformation is the set of dialectical processes intentionally put into play in order to succeed in the treacherous manipulation of individuals, groups or an entire society in order to deviate them from political conduct, to dominate their way of thinking or even to subjugate them"*[13];
- *"disinformation is the manipulation of the public opinion (not individuals) for political purposes (otherwise it could be propaganda) of truthful information, or not (it is not the truthfulness of the information that matters but the way it is presented)"*[14];
- *"manipulation is an instrument of disinformation, along with intoxication, propaganda, influence, lying, tactical cunning, subversion and diversion"*[15].

Disinformation existed in some armed confrontation because some military commanders were interested in hiding from their adversary the data regarding their own troops that they considered to be vulnerabilities (weaknesses), but also to watch over his strengths (centers) and intentions.

It may seem paradoxical, but disinformation is disheartened, even rejected, by the moral norms of the society because, in the vast majority of cases, it is associated with the lie, but in the armed confrontations it is accepted by both International Law, which considers it a *"war stratagem"*[16] as well as the military regulations that define it by the phrase *"military deception ..... [meant] to contribute to the fulfillment of the mission"*[17].

Disinformation existed in some armed confrontation because some military commanders were interested in hiding from their adversary the data regarding their own troops that they considered

[11] Călin Hentea, *Noile haine ale propagandei*, Editura Paralela 45, București, 2008, p. 59.
[12] *Ibid*.
[13] Henri Pierre Cathala, *Epoca dezinformării*, Editura Militară, București, 1991, p. 24.
[14] Vladimir Volhov, *Dezinformarea văzută din Est*, Editura ProEditură și Tipografie, București, 2007, p. 24.
[15] Ştefan Stanciugelu, *Logica manipulării*, Editura C.H. Beck, București, 2010, p. 64.
[16] Ion Dragoman, *Drept internaţional umanitar*, Fundaţia Andrei Şaguna, Constanţa, 1999, p. 69.
[17] *Doctrine for Information Operations*, Joint Pub 3-13, February 1998, United States of America.

to be vulnerabilities (weaknesses), but also to watch over his strengths (centers) and intentions.

Historians have recorded famous acts of disinformation (deception) such as:

- The Gleiwitz incident, which was the pretext for the outbreak of World War II – 1 September 1939[18];
- the moment of the aggression against the USSR – Operation Barbarossa – in the Second World War – 22 June 1941;
- the Japanese attack at Pearl Harbor on the US Pacific Fleet – 7 December 1941 – and the outbreak of the Pacific War between Japan and the US;
- the place and time of the Allied landing, in World War II – June 6, 1944, Normandy;
- relocation and installation of Soviet medium-range missiles in Cuba (1962)[19] – during the Cold War;
- the changed perception over Serbian leader Slobodan Milosevich and the Serbian people, before the Kosovo war broke out[20];
- influencing American public opinion and part of the international community to support the outbreak of the second Gulf War and to halt Iraqi weapons of mass destruction development programs[21].

ROMANIAN MILITARY THINKING

The causes of the crisis in Ukraine are manifold, both internal (poor economic performance, political and ethno-linguistic division), and external (influence of the population by Russia in order not to accept the country's integration into the Euro-Atlantic organisations, influence of the population by the West to eliminate corruption and the development of democracy, with a view to the integration into Euro-Atlantic organisations).

THE USE OF DISINFORMATION IN THE HYBRID WAR IN UKRAINE

The causes of the crisis in Ukraine are manifold, both internal (poor economic performance, political and ethno-linguistic division), and external (influence of the population by Russia in order not to accept the country's integration into the Euro-Atlantic organisations,

[18] Dennis Whitehead, *The Gleiwitz Incident*, in *"After Battle Magazine"*, no. 142, March 2009 (http://en.wikipedia.org/Gleiwitz_incident/, retrieved in November 2019.
[19] Igor A. Amosov, Captain First Rank (ret.) Professor, Ph. D., *Caribbean Missile Crisis, 1962 – The World on the Brink of Nuclear Catastrophe*, in colonel dr. Petre Otu, colonel Gheorghe Vartic, locotenent-colonel dr. Mihai Macuc (coord.), On Both Sides of the Iron Curtain, Editura Militară, București, 2001, pp. 237-246.
[20] Simona Ştefănescu, *Media şi conflictele*, Editura Tritonic, București, 2004, pp. 194-218.
[21] Alexandru Ioan, *Între putere şi democraţie. Presa în politica internă şi internaţională*, Editura Centrului Tehnic-Editorial al Armatei, București, 2017, pp. 145-158, see also Tim Weiner, *CIA, O istorie secretă*, Editura Litera Internaţional, București, 2009, pp. 355-356 şi 364-366.

influence of the population by the West to eliminate corruption and the development of democracy, with a view to the integration into Euro-Atlantic organisations). Against this backdrop of internal contradictions and external influences, Ukraine has become a space of confrontation between Russia and the West[22].

In order to support its declared interests (supporting the Russian population in eastern Ukraine and stopping NATO expansion to the east) and undeclared (regaining the status of world superpower and the possible restoration of the USSR), the leadership of the Russian Federation launched extensive actions to influence the Ukrainian population., but also the international community through manipulation and disinformation. The disinformation initiated by Moscow was supported by decisions in the political, diplomatic, economic, financial, cultural, informational and military plans, that were disseminated throughout the world through a highly developed and performing media apparatus. The actions of Kremlin are considered hybrid warfare specific actions by most Western specialists and Euro-Atlantic organisations.

The disinformation initiated by Moscow was supported by decisions in the political, diplomatic, economic, financial, cultural, informational and military plans, that were disseminated throughout the world through a highly developed and performing media apparatus.

The disinformation campaign against the Ukrainian population, carried out by the Russian leadership, evolved mainly upwards, in terms of magnitude and intensity, after 2000, when President Vladimir Putin came to lead the Federation. Among the most important and extensive disinformation campaigns, carried out until the onset of the current crisis in Ukraine, are those aimed at influencing the 2004 and 2010 presidential elections.

If in 2004 the Russian campaign of influence prevailed over the pro-Russian Viktor Yanukovych, popular protests, generated by pro-Western militants, led to the resumption of the electoral process and the victory of candidate Yushchenko[23], the man who wanted to direct the country to NATO and the EU and to cause the withdrawal of Russian military forces from the Crimean Peninsula.

[22] Mihail Orzeaţă, *Ucraina – spaţiu de confruntare între Rusia şi Occident*, in Eugen Lungu, coordinator, *Federaţia Rusă şi echilibrul de putere în secolul al XXI-lea*, pp. 95-127, Editura Militară, Bucureşti, 2019.

[23] Malin Ostevik, *Communicating Conflict: Russian Mediated Public Diplomacy in Relation to the Annexation of Crimea*, University of Oslo, May 2016, p. 21.

ROMANIAN MILITARY THINKING

In 2010, Viktor Yanukovych ran again, backed by Moscow, and won the chair of the President of Ukraine. From this position, Viktor Yanukovych signed the extension of the Russian-Ukrainian agreement on the stationing of the Federation forces in Crimea until 2017 and the loan agreement of 15 billion USD from Russia, in package with the agreement to reduce the Russian natural gas, delivered to Ukraine. Although the details of the negotiations for these agreements were not officially communicated, unofficial but well-informed sources revealed the Kremlin's condition imposed to Yanukovych not to sign the Association Agreement with the EU.

In 2010, Viktor Yanukovych ran again, backed by Moscow, and won the chair of the President of Ukraine. From this position, Viktor Yanukovych signed the extension of the Russian-Ukrainian agreement on the stationing of the Federation forces in Crimea until 2017 and the loan agreement of 15 billion USD from Russia, in package with the agreement to reduce the Russian natural gas, delivered to Ukraine.

President Yanukovych complied about the condition imposed by the Moscow leadership and did not sign the agreement with the EU, but his gesture sparked massive protests in Kiev and then across the country. The protests have degenerated into violent clashes with law enforcement, prompting President Yanukovych to take refuge in Russia in February 2014 and call on his Russian counterpart to intervene militarily to save the country from undemocratic forces.

Against this background of political instability, street violence and tendencies towards authoritarianism, promoted by right-wing forces, the Moscow leadership intensified the disinformation campaign towards the Ukrainian population, the international community and its own population. In this way, it achieved several notable successes, such as:

- the annexation of the Crimean Peninsula (18 March 2014[24]), without firing any fire, but benefiting from the support of the Russian ethnic population from the peninsula and from the actions of some military members without insignia of belonging, previously infiltrated in the strategic areas and several tens of thousands of combat-equipped soldiers stationed on the border with Ukraine to *"prevent the infiltration of extremist elements into Russia"*;

[24] Ilya Somin, *Russian Government Agency Reveals Fraudulent Nature of the Crimean Referendum Results*, in *The Washington Post*, 6 April 2014, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/06/russian-government-agency-reveals-fraudulent-nature-of-the-crimean-referendum-results/ retrieved in 2020.

- supporting the secession of the Lugansk and Donetsk regions, populated mostly with Russian ethnic groups, self-proclaimed republics, under the pretext of an intention to exterminate (alienate) the Russians from Ukraine, an intention attributed to former Ukrainian Prime Minister YuliaTymoshenko[25];
- gaining the trust of the majority of the Russian population in Ukraine, which voted for the integration of self-proclaimed republics in the Russian Federation;
- the ascension of its status in international relations, a status maintained by the other members of the BRICS group (Brazil, Russia, India, China, South Africa), but also by the states in conflict with the US and some western states;
- attempting to destabilise NATO by approaching Turkey, to which it sells S-400 ground-to-air missiles, leading to the exclusion of Ankara from the F-35 program[26];
- the efforts of the Russian Federation to break the economic-financial blockade, established by the European Union against it, materialized in bilateral economic-financial relations with Hungary, Slovakia, the Czech Republic, Germany and Bulgaria[27].

The efforts of the Russian Federation to break the economic-financial blockade, established by the European Union against it, materialized in bilateral economic-financial relations with Hungary, Slovakia, the Czech Republic, Germany and Bulgaria.

CONCLUSIONS

Disinformation is a method of influencing large masses of people, in a declarative plane, by political personalities and by states, which is used quite often in subversive campaigns, meant to lead, by any means, to the achievement of great objectives.

The Internet, through the social networks and the classical mass media[28], has greatly contributed to the increase in the scope and efficiency of the manipulation and disinformation campaigns[29]. Lately, the media in general, and opinion formers in particular, have played an important role in disseminating false information. Thus, there has been a significant increase in the number of news programs that amplify prefabricated and exaggerated narratives.

With the development of artificial intelligence technologies, disinformation campaigns have become much more sophisticated and better organised, in order to direct citizens' attention to preconceived narratives, to discredit political opponents, and to counteract different opinions.

In an information environment oversaturated with false information, preconceived narratives that appeal to personal prejudices are very accessible. Some researchers in the field have associated preconceived narratives with epidemics, respectively the spread of preconceived narratives is similar to the spread of viruses. They transcend the information space, moving from one cognitive system to another. Therefore, the problem is not irrational trust, but it concerns a much deeper aspect, namely the systems of personal beliefs that determine decisions and form prejudices. Thus, experts claim that the human cognitive system perceives the world around it as divided into objects located in space and time, but is not always able to faithfully reproduce its shape.

The disinformation campaigns carried out by the Russian Federation against the Ukrainian population and the international community have brought it numerous international criticisms and sanctions, mainly from Western states, but they have also generated an upward course of its status in the international arena which was indirectly recognised through the accusations of influencing the presidential election in the United States of America. The rise of the Russian Federation in the international arena is facilitated by the increase of anti-globalisation, anti-Western and anti-American currents and feelings.

With the development of artificial intelligence technologies, disinformation campaigns have become much more sophisticated and better organised, in order to direct citizens' attention to preconceived narratives, to discredit political opponents, and to counteract different opinions.

[25] Mark Thompson, *Russian Forces Double Along Ukraine Border*, in *Time*, 28 March 2014, http://time.com/41490/russia-ukraine-crimea-putin/, retrieved in November 2019; see also Maria Dejovsky, *News of a Russian Arms Buildup Next to Ukraine Is Part of Propaganda War*, in *The Guardian*, 11 April 2013, http://www.theguardian.com/commentsisfree/2014/apr/11/russian-arms-buildup-ukraine-propaganda-war-nato/, retrieved in November 2019.

[26] Ted Galen Carpenter, *Is It Time to Expel Turkey from NATO?*, in *The National Interest*, https://nationalinterest.org/blog/the-skeptics/it-time-expel-turkey-nato-14518, retrieved in September 2019, see also Burak Bekdil, *Turkey: Putin's Ally in NATO?*, Gatestone Institute, 19 March 2019, https://www.gatestoneinstitute.org/13882/turkey-putin-ally-nato, retrieved on September 2019.

[27] Tatia Dolidze, *EU Sanctions Policy towards Russia: The Sanctioner-Sanctionee's Game of Throne*, CEPS Working Document, Center for European Policy, No. 402, pp. 8-9, January 2015, http://www.ceps.be/system/files/WD%20402%20TD%20Sanctions.pdf, retrieved on 10 April 2015.

[28] Sonia Cristina Stan, *Manipularea prin presă*, Editura Humanitas, București, 2004, pp. 35-36.

[29] Vladimir Volhov defines television as a *"paradise of misinformation"*, in a world where cybernetics is a real Olympus and the internet the *"trade plains"* of disinformation Vladimir Volkoff, *Tratat de dezinformare. De la calul troian la internet*, Ed. Antet, ISBN 973-9241-87-5, p. 213.

BIBLIOGRAPHY

1. ***, *Doctrine for Information Operations*, Joint Pub 3-13, February 1998, United States of America.
2. ***, *Time to Grab and Kill Damn Russians – Timoshenko in Leaked Tape*, *Russia Today*, 24.03.2014, http://rt.com/news/tymoshenko-calls-destroy-russia-917/.
3. Madeleine Albright, *Who Broke the U.N.*?, *Foreign Policy*, 13.08.2012, http://foreignpolicy.com/2012/08/13/who-broke-the-u-n/.
4. Zygmunt Bauman, *Globalizarea și efectele ei sociale*, Editura Antet, Oradea.
5. Henri Pierre Cathala, *Epoca dezinformării*, Editura Militară, București, 1991.
6. Roberta Cohen, *The Role of Regional Organizations*, ECOWAS, Brookings, Monday, 30 September 2002, https://www.brookings.edu/on-the-record/the-role-of-regional-organizations-ecowas/
7. Ion Dragoman, *Drept internațional umanitar*, Fundația Andrei Șaguna, Constanța, 1999.
8. Călin Hentea, *Noile haine ale propagandei*, Editura Paralela 45, București, 2008.
9. Alexandru Ioan, *Între putere și democrație. Presa în politica internă și internațională*, Editura Centrului Tehnic-Editorial al Armatei, București, 2017.
10. Majid Khadduri, *War and Peace in the Law of Islam*, John Hopkins University Press, Baltimore, 1955, *apud* Dr. Lewis B. Ware, *An Islamic Concept of Conflict in Its Historical Context*, Blank, Stephen J, Grinter, Lawrence E., Magyar, Karl P., and Wheaters, Bynum E., *Conflict, Culture and History*, Air University Press, Maxwell Air Force Base, Alabama, SUA, 1993.
11. Irina Moroianu Zlătescu, *Drepturile omului – un sistem în evoluție*, Institutul Român pentru Drepturile Omului, București, 2017.
12. Mihail Orzeață, *Războiul continuu*, Editura Militară, București, 2011.
13. Mihail Orzeață, *Suntem pregătiți pentru războiul viitorului?,* in *Gândirea Militară Românească* Journal, no. 4 (October-Deceber), 2016.
14. Mihail Orzeață, *Ucraina – spațiu de confruntare între Rusia și Occident*, in Eugen Lungu, coordonator, *Federația Rusă și echilibrul de putere în secolul al XXI-lea*, Editura Militară, București, 2019.
15. Malin Ostevik, *Communicating Conflict: Russian Mediated Public Diplomacy in Relation to the Annexation of Crimea*, University of Oslo, May 2016.
16. Sonia Cristina Stan, *Manipularea prin presă*, Editura Humanitas, Bucureşti, 2004.
17. Ștefan Stanciugelu, *Logica manipulării*, Editura C.H. Beck, București, 2010.

18. Silvia Șpac, *Impactul mass-media asupra formării personalității elevului de vârstă școlară mică*, Studia Universitatis Moldaviae, 2015.
19. Simona Ștefănescu, *Media și conflictele*, Editura Tritonic, București, 2004.
20. Paul Virilio, *Un monde surexposé: fin de l'histoire ou fin de la geographie?,* in *Le monde diplomatique*, August 1997.
21. Vladimir Volhov, *Dezinformarea văzută din Est*, Editura ProEditură și Tipografie, București, 2007.
22. Dennis Whitehead, *The Gleiwitz incident*, in *"After Batle Magazine"*, nr. 142, March 2009, http://en.wikipedia.org/Gleiwitz_incident/.

ENVIRONMENTAL PROTECTION IN THE EVENT OF ARMED CONFLICTS

Mădălina Virginia ANTONESCU

PhD in European Law, Scientific Researcher – University of Bucharest

The present article explores a topical area of the relationship between the environment, the rights of the future generations to enjoy a clean, healthy and safe environment, unaffected by wars, as well as the right of future generations to live in a world free of terror, poverty and insecurity. There are some international regulations regarding the relationship between the environment and military technologies or those technologies used for hostile purposes, but they need to be improved and correlated with the recent developments related to the obligations of states in terms of sustainable development and environmental protection. The environment should be protected not only in relation to the right of peoples and states to development but also in relation to the military conflicts and any type of crises that entail destructive technologies. We consider it as an area of major interest in which, starting from the definition of the "environment manipulated for military purposes", it is possible to develop studies on comparative law and security related to this legal relationship.

Keywords: international environmental law, Global Pact for the Environment, European Green Pact, security threats, military technologies.

THE ENVIRONMENT PER SE IS NOT A MILITARY OBJECTIVE AND CANNOT BE CONSIDERED AS SUCH

Environmental security is, in the 21st century, part of national, European, regional and international security. The environment is becoming increasingly important in the legal and political culture of 21st century societies because of the challenges related to climate change, intensification of industrialisation, air and water pollution, increasing deterioration of soil and subsoil quality, continuing modification of natural ecosystems and global link between all terrestrial ecosystems, which are in a fragile balance.

The responsibility of human societies on the quality of life on Earth, on the preservation of natural ecosystems starts to be seen as part of a specific concept, *"environmental security"*, which becomes part of the concept of national, regional-European and international security.

The responsibility of human societies on the quality of life on Earth, on the preservation of natural ecosystems starts to be seen as part of a specific concept, "environmental security", which becomes part of the concept of national, regional-European and international security.

Regardless of the perspective on the concept of *"environmental security"*, it is no longer an isolated one, but one closely related to hitherto classic terms in their meaning (national, regional, international security).

The impairment of the quality of the environment in one state can create effects in another state, therefore environmental security should be considered in terms of cross-border security, for which mechanisms, strategies, institutions for environment-related crisis and disaster prevention and management should be designed.

Currently, the development of military technologies should not affect the environment, as their degree of *"intelligence"* (high-precision strike) is increased. In both military strategies and tactics, environmental protection should be seen as a form of accountability to preserve the planet's natural heritage for future generations.

In other words, the increasingly development of technology and *Artificial Intelligence (AI)* in the nature of military armaments and in the way of conceiving and waging wars in the 21st century must start from the mandatory premise of environmental protection, from *defining*

it as not being a military objective, from the obligation of present generations, whatever the differences between them, to preserve a healthy planet, rich in functioning and healthy natural ecosystems, an increased quality of life, for future generations.

The right of future generations to a healthy environment[1], to a high quality of life starts to become a fundamental right not only of the *man* but also of the *mankind* (another legal concept already considered by the legal practitioners in the 21st century).

The increasingly development of technology and Artificial Intelligence (AI) in the nature of military armaments and in the way of conceiving and waging wars in the 21st century must start from the mandatory premise of environmental protection, from defining it as not being a military objective, from the obligation of present generations, whatever the differences between them, to preserve a healthy planet, rich in functioning and healthy natural ecosystems, an increased quality of life, for future generations.

Today, we can say that we are witnessing, once again, an *arms race*, because of a specific view of the global world, a technological leap in terms of weapons, doubled by both the *ineffectiveness of disarmament regulations and the recent practice of withdrawal of major states from international agreements*.

Through their very existence, the types and quantities of weapons owned by states today represent *direct and serious threats to the planet, the natural ecosystems and the environment in any state*, according to the doctrine[2]. The existence of stockpiles of weapons of mass destruction, able to destroy the environment as well as urban settlements and targets, generates ecological imbalances as the doctrine has already noted[3].

The International Environmental Law has been influenced by the relationship between the environment and armed conflicts, thus being necessary to regulate the juridical concept of *"environment manipulated for military purposes"*. It has been defined as the type of environment *"whose composition, structure and dynamics are disrupted by the use of means and methods of warfare, including environmental manipulation techniques"*[4]. Therefore, the doctrine uses an updated definition of the concept, introducing, among the military technologies that violently affect the environment (armed conflicts, wars), *the military (or employed for military purposes) techniques to disrupt the environment*. This conception of the legal doctrine in the matter also includes *the systems used to influence or disrupt*

[1] See https://www.un.org/en/universal-declaration-human-rights/, retrieved on 18 February 2020.
[2] Daniela Marinescu, *Tratat de dreptul mediului*, IVth edition, Editura Universul Juridic, București, 2010, pp. 600-601.
[3] *Ibidem*.
[4] *Ibidem*.

the climate or the weather (the so-called military technologies employed in the environmental warfare)[5].

The *"environment manipulated for military purposes"* is a concept that increasingly develops in the 21st century, in line with the military and civilian technological progress, and with the possibility for it to be used by state or non-state actors (terrorist networks, organisations etc.) in wars, armed conflicts, crises or to trigger or extend such crises.

The *"environment manipulated for military purposes"* can be exposed to the intervention of military or civilian techniques in the event of armed conflicts or of any type of local or regional crises, with the *employment of some non-state or supra-state actors* (militias, security forces, paramilitary troops, troops of rival generals in failing or dissolving states etc.).

The *"environment manipulated for military purposes"* can be subjected not only to the intervention of categories recognised by public international law (peoples fighting for independence, belligerents, military forces representing states or alliances of states) but also to the intervention (unauthorised, non-legitimate from the perspective of public international law) of non-state actors (terrorist networks, armed religious groups etc.).

However, in our opinion, we should not consider that since an actor has the status of subject of public international law, it has the *"legitimacy"* to destroy the environment through the employed military techniques and technologies or through those used for military purposes.

The environment must not become or be treated as a military objective, because it is the essential element for the survival of the human species, being composed of the set of unique ecosystems, dependent on each other, and arranged globally in an interconnected way. In other words, the responsibility of states in the 21st century, which is intended to be a century of advancement in technique, technology and science (including in the military field and in the concept of war or military conflict), must include, from a legal and political point of view, at national, regional and global level, a direct responsibility for the environment.

ROMANIAN MILITARY THINKING

The "environment manipulated for military purposes" can be subjected not only to the intervention of categories recognised by public international law (peoples fighting for independence, belligerents, military forces representing states or alliances of states) but also to the intervention (unauthorised, non-legitimate from the perspective of public international law) of non-state actors (terrorist networks, armed religious groups etc.).

[5] *Ibidem*, p. 601.

States should expressly assume, through national, regional (European, for example) as well as international law, the obligation to *deter any action* by any other state or non-state actor in damaging or affecting, through military or civilian techniques and technologies used for military purposes, the quality and the *very existence* of the ecosystems *on their territory* and on that they undertake their responsibility according to the principles and norms of international and national environmental law.

The sovereignty of the state also entails its sovereignty over its territory, over all natural and artificial ecosystems within the limits of its jurisdiction.

The state, in a Westphalian order, continues to remain the main actor and subject of international environmental law that will take responsibility for the violent intervention on the environment (in the event of armed conflicts, war or any terrorist or other non-state or quasi-state groups act) and for allowing or not preventing the intervention or not restoring the environment affected by such an intervention.

The state, therefore, in a Westphalian order, continues to *remain the main actor and subject of international environmental law that will take responsibility for the violent intervention on the environment* (in the event of armed conflicts, war or any terrorist or other non-state or quasi-state groups act) and for allowing or not preventing the intervention or not restoring the environment affected by such an intervention.

Moreover, a regional or international legislation adapted to the 21st century as a century of global interdependence (in which, if an ecosystem in a region is affected by an armed intervention of any kind, harmful effects on the quality of life and the environment in other states or regions are created) should provide *for strengthened obligations of solidarity of states at regional and international level and mechanisms, clear collective procedures, to be activated in such cases*, where military interventions of any kind produce disasters or serious effects on the environment of a country or a region .

In the 21st century, due to the increasing destructive potential of military technologies and techniques, the degree of the legal responsibility of states for the destruction or non-repair of the environment manipulated for military purposes must also increase accordingly.

We would even say that in the century of climate change, when we are already talking about climate wars, in line with the military technological advance of states, the concept of *"environment manipulated for military purposes"* becomes extremely important to provide legal and political guarantees for world peace and the right of present and future generations to peace, to a high quality of life.

To date, *two general principles* are considered to be included in international environmental law (however, this is an area that needs to be *constantly adapted and improved*). The first principle takes into account the obligations of each state (being therefore limited to the sphere of state actors, although military interventions, regardless of their name, can be also carried out by non-state actors) *not to cause environmental damage beyond its territorial competence*. Belligerents are not exempt from this obligation, as they are liable for cross-boundary damage caused to the natural environment[6]. However, there may be a legal obligation in the future for belligerents to take responsibility in case of cross-border or sub-local damage caused to the *artificial environment* (urban settlements, villages) or the *mixed environment* (parts of the natural environment integrated into the urban or rural environment), such as those on the outskirts of large cities or in any space surrounding a group or an urban or rural settlement. This would be an *extension of the obligations of legal liability in the case of belligerents*, which would apply mainly to states (therefore, not only in the case of the *natural environment* affected by military technologies).

To date, two general principles are considered to be included in international environmental law. The first principle takes into account the obligations of each state not to cause environmental damage beyond its territorial competence. The second principle concerns the obligation of states to respect the environment in general.

The second principle concerns the *obligation of states to respect the environment in general*. As we can see, this is also a principle related to *states*, so a limited one, while, in reality, irreparable damage or destruction can be caused to the environment by military manipulation not only by states but also by *non-state or quasi-state actors.*

This second principle concerns the obligations of states to respect the environment and not to damage it outside their jurisdictions, for example in the open sea areas, on the bottom of the seas and oceans, in areas of common interest for humanity, such as the Moon, the Cosmos, the open sea, Antarctica or celestial bodies[7].

In other international documents adopted under the auspices of the UN, for example in the World Charter for Nature[8], there are stipulated principles that must be respected by *states*, connected to the principle

[6] Daniela Marinescu, *op. cit.*, p. 601.
[7] *Ibidem*, p. 601.
[8] See https://www.refworld.org/docid/3b00f22a10.html, retrieved on 12 February 2020.

of sustainable development. These principles, as they are included in the Charter, make it an important document for defining the legal order of the 21st century as a legal order based on the responsibility of states towards the environment and on the mandatory compliance of their development policies with the environmental protection requirement. The principles are as follows:

- principle of respect for nature and its natural processes, states being expressly obliged not to affect or prevent them (hence, including a legal obligation applicable in the event of armed conflicts or crises that entail, regardless of their name or type, military or civilian technologies used for military purposes or having a violent impact on the environment);
- principle of conservation of biodiversity and habitats that are necessary to preserve biodiversity, principle of management or use of ecosystems and organisms, land, marine and atmospheric resources from the perspective of sustainability and integrity of such ecosystems or species;
- principle of conservation of all areas of the Earth, land or water, a special protection being given to unique areas and to rare or endangered species[9].

In the World Charter for Nature it is expressly stipulated, related to the present topic, the principle of protecting nature against the degradation caused by wars or other hostile activities.

In the World Charter for Nature *it is expressly stipulated, related to the present topic, the principle of protecting nature against the degradation caused by wars or other hostile activities.*

States also have, through point 21 in the Charter, legal obligations as follows:

- to cooperate for the conservation of nature, through joint activities, consultations, exchange of information;
- to establish the standards for the products and manufacturing processes that *can produce adverse effects on nature*;
- to implement the international legal provisions related to environmental protection and conservation;
- to ensure that the *activities under their jurisdiction or control* will not cause damages to the natural systems located *in other states or areas beyond* national jurisdiction;

[9] *Ibidem.*

- to protect, save and conserve nature *in areas beyond* their national jurisdiction. This point in the Charter *extends the scope of legal responsibility not only to states but also to international organisations*, which are explicitly specified for the fulfilment of the above-mentioned obligations.

Art. 5 in the World Charter for Nature expressly refers to the principle according to which nature will be protected from the degradation caused by war or other hostile acts, and Art. 20 requires states to *avoid the military activities that can cause damage to nature*[10]. These two provisions are imperatively addressed to states, which are subjects of international law. Consequently, *states must guarantee* environmental protection in the event of hostile acts or wars, *eliminating these dangers and degradations* that may be caused or about which there are clear indications that will be indirectly or directly caused by the action of non-state actors. This *legal extension to the two principles*, regarding the responsibility of states for the degradations generated or potentially generated by non-state, quasi-state actors (in regions where the authority of states is weakened, or dissolved, or no longer exists), *is necessary*, we consider, and *it should be swiftly included* in regional and international environmental protection documents.

Art. 5 in the World Charter for Nature expressly refers to the principle according to which nature will be protected from the degradation caused by war or other hostile acts, and Art. 20 requires states to avoid the military activities that can cause damage to nature.

Moreover, we also consider necessary the implementation of the *principles of good neighbourliness and regional solidarity of states,* in the event a state is dissolving or failing, its authority being contested by the non-state actors that act on its territory (the case of Syria, Libya, Iraq, Yemen), where it is required either a collective responsibility of the states participating in the military conflict on that territory, the neighbour states, or the international community in its aggregate, to restore and protect the environment affected by the military activities conducted on that territory.

The case of the territories in a state of dissolving or failing, because of an armed conflict in which other states as well as non-state actors are involved (paramilitary, terrorist, rebel, militia and other groups), *urgently requires a legal regulation for the protection of the environment manipulated for military purposes in such cases*, at both regional and international level, imposing direct responsibility

[10] Daniela Marinescu, *op. cit.*, p. 601.

for the quality of the environment of the states participating in the armed conflict as well as the responsibility of the participating states for the military interventions of the non-state groups.

Such responsibility should also be met in the case of protecting and restoring the objects or sites representing *cultural heritage* on the territory affected by armed conflicts.

The *"environment manipulated for military purposes"*, in its broad sense, as it should be sanctioned in a future international convention, *should include not only the natural environment per se but also the artificial environment (urban), mixt (outskirts of a settlement, its periphery, surrounding areas), but also the cultural environment (tourist, historical, cultural sites).* These types of environments should be protected from military interventions, free from destruction, and national, regional and international sanctioning legislation should be adopted to protect them, regardless of the type of environment.

The "environment manipulated for military purposes", in its broad sense, as it should be sanctioned in a future international convention, should include not only the natural environment per se but also the artificial environment (urban), mixt (outskirts of a settlement, its periphery, surrounding areas), but also the cultural environment (tourist, historical, cultural).

It should also be mentioned the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD*), adopted by the UN General Assembly on 10 December 1976 and entered into force on 5 October 1978[11]. Romania signed the Convention on 18 May 1977 and ratified it through the Decree no. 100 on 28 March 1983. This international legal instrument has unlimited validity and converts, in our opinion, into a preliminary and mandatory legal framework for not only states but also, by extension, for non-state actors, in order to ensure an environmental protection appropriate to the 21st century. We also mention here that the text of the Convention establishes an Advisory Committee at expert level, which can be convened ad-hoc upon the request of states parties. The competence of this Committee is to provide official consultations related to possible disputes and to exactly determine the nature of the activities suspected of violating the Convention[12]. Other provisions of the Convention concern the manner in which the delegates of states parties can meet during periodical conferences to review the functioning of the Commission. In this context, it should be

[11] See file:///C:/1976-enmod-icrc-factsheet.pdf, https://www.unog.ch/enmod, retrieved on 12 February 2020.

[12] Adrian Năstase, *Documenta universales I, Documente fundamentale ale dreptului internațional contemporan și ale relațiilor internaționale,* Roxana Frailich (editor), Asociația Română pentru Educație Democratică, Regia Autonomă Monitorul Oficial, București, 1997, p. 408.

noted that the USA is also party to the Convention, the president ratifying the Convention on 13 December 1997, it entering into force for the USA on 17 January 1980, when the instrument of ratification was deposited in New York[13].

This Convention is of essential importance for the relationship between the environment and military activities, *banning the use of new methods or means of combat intended to produce or which are expected to produce widespread, long-lasting harmful effects* in relation to the environment.

The Convention *also prohibits techniques with widespread, long-term or serious effects on the environment*. It is appreciated that the *very existence* of new techniques, likely to harm or modify the environment for military purposes, may be the beginning of serious disasters, if the process escalates[14], as it is stated in the Convention.

The Convention *defines environmental modification techniques as "altering – along with deliberate changes in natural processes –, the dynamics, composition, structure of air, including the biosphere, atmosphere, lithosphere, hydrosphere or outer space, by producing earthquakes, avalanches, landslides etc."*[15].

The convention is of essential importance for the relationship between the environment and military activities, banning the use of new methods or means of combat intended to produce or which are expected to produce widespread, long-lasting harmful effects in relation to the environment.

The Convention considers as examples of the negative effects that could result from the use of environmental modification techniques the following: climate or climate agents change, ecological upheaval, changes in ocean currents, changes in the ozone layer or ionosphere.

For the time at which it was signed and ratified (1970s-1980s), the Convention is of unexpected innovative value in a field which, decades later, has hitherto been regarded as vital to the survival of the human species, and of the planet itself.

Today, climate change generates wide and deep debates related to different visions of states, for and against the abandonment of technologies and economies with large or particularly intense disruptive potential (due to the degree of industrialisation, chemical agriculture, massive deforestation etc.) to the environment. There is a close link between climate change and human intervention (here, of the state,

[13] *Ibidem*, p. 409.

[14] See file:///C:/1976-enmod-icrc-factsheet.pdf, https://www.unog.ch/enmod, retrieved on 12 February 2020.

[15] *Ibidem.*

of companies, in particular) and the capacity of the environment to regenerate. The Convention expressly refers, in its preamble, to the *Declaration of the United Nations Conference on the Environment*, in Stockholm, on 16 June 1972 and recommends the *peaceful use* of environmental modification techniques, expressly mentioning *the right of present and future generations to benefit from a preserved and enhanced environment*.

The Convention (63 signatory states) acknowledges the extremely damaging effects the use of such techniques for military or other hostile (therefore, a broad definition, including *any action having a hostile to environment character, not only the military ones* to manipulate the environment) purposes may have on the environment.

Art. 1 in the Convention introduces in the responsibility of the signatory states the obligation of not getting engaged in the use of any technique to modify the environment for military or other hostile purposes, having large-scale, long-lasting or severe effects, as means of causing destruction, damage, or injury to other states parties.

Art. 1 in the Convention introduces in the responsibility of the signatory states the *obligation of not getting engaged* in the use of any technique to modify the environment for military or other hostile purposes, having large-scale, long-lasting or severe effects, as means of causing destruction, damage, or injury to *other states parties.* In paragraph 2, such a prohibitive provision for the states parties is also extended to their *relations with third parties* (other states, groups of states or international organisations), states parties undertaking *not to assist, to encourage, or to incite* other states, groups of states or international organisations to engage in activities contrary to paragraph 1. This is a provision having *broad and extremely important applicability*, based on the provision for the states parties to *preserve the environment and not to use it for military or any other hostile purposes, not only in the relations between them, but also in those with third parties, whether they are states, groups of states (alliances, coalitions, federations) or international organisations*. Other categories (non-state actors) that have proliferated in the last two decades at the infra-local, regional and even global levels are not included in this Convention, but the *text can be extended and improved*.

Article IV obliges signatory states to take any measure deemed necessary to prohibit or prevent any activity contrary to this Convention, in *any place* under their jurisdiction or control.

Moreover, according to Art. 5 of the Convention, states parties are obliged to *cooperate and consult with each other* in order to resolve any problem that may arise in connection with the objectives

of this Convention or its application. Cooperation activities within the UN and its organisations are also encouraged.

If a state party considers that any other state party is in breach of its obligations under this Convention, it may lodge a complaint with the UN Security Council which has jurisdiction to investigate, in accordance with the UN Charter, the facts resulting from the complaint received by the Council. If the UN Security Council decides that the party concerned has been harmed or is at risk of injury as a result of a violation of this Convention, each state party shall be obliged to provide assistance or support to any party to the Convention that requests it. Article VI introduces a *legal possibility to extend the content of the Convention by submitting amendments by states parties*.

The recently adopted documents under the aegis of the UN repeatedly refer to the right of humans to a healthy and balanced environment, to the rights of peoples and future generations to a high quality of life, which can be achieved only if the environment quality is preserved, respected and enhanced.

INTERNATIONAL AND EUROPEAN DOCUMENTS RELATED TO THE RELATIONSHIP BETWEEN THE ENVIRONMENT AND SECURITY THREATS

The recently adopted documents under the aegis of the UN repeatedly refer to the right of humans to a healthy and balanced environment, to the rights of peoples and future generations to a high quality of life, which can be achieved (as the right to sustainable development, another fundamental right, among the most recent categories of human and people rights in the past decades) only if the environment quality is preserved, respected and enhanced. Among these documents (***that have legal incidence on the relationship between the environment and the armed conflicts***, introducing *indirect obligations* for states regarding environmental protection, including in terms of using technologies for military or other hostile purposes), we can list: UNGA Resolution on Harmony with Nature (A/RES/67/214); UN Secretary-General Report on Harmony with Nature (A/67/317); UN Secretary-General Report on Harmony with Nature (A/66/302); UNGA Resolution on Harmony with Nature (A/RES/65/164); UNGA Resolution on Harmony with Nature (A/RES/64/196); Study on the need to recognise and respect the rights of Mother Earth (E/C/2010/4); UNGA Resolution on Mother Earth International Day (A/RES/63/278); UNGA Resolution on Planet Earth International Year, 2008 (A/RES/60/192), supplemented by Agenda 21 or documents developed under the auspices of ECOSOC[16].

[16] See http://www.un.org/en/events/motherearthday/documents.shtml, retrieved on 7 September 2016.

As far as the relationship between the use of technologies for military or other hostile purposes and their impact on the environment, another international document should be mentioned, namely the *Johannesburg Declaration on Sustainable Development* on 4 September 2002[17]. It was adopted following the World Summit on Sustainable Development in South Africa (2-4 September 2002), acknowledging the *responsibility of present generations for the level of civilisation and welfare of future generations, as well as for the quality of life on Planet Earth* (states parties assuming certain obligations related to the preservation of terrestrial ecosystems). Point 13 (global challenges related to environment) also mentions the continuous degradation of global environment, by continuous loss of biodiversity, by *adverse effects of climate change (which can be produced inclusively by technologies used for military purposes or other purposes that are hostile to the environment and the society)*.

According to the UNGA Resolution on 22 April 2009, which establishes Planet Earth International Day on 22 April every year, the UN member states are recommended to adopt in their policies "a harmonious relationship with nature and the Earth, to achieve a fair balance between the economic, social and environmental needs of present and future generations".

According to the UNGA Resolution (A/RES/63/278) on 22 April 2009, which establishes Planet Earth International Day on 22 April every year[18], the UN member states are recommended to adopt in their policies *"a harmonious relationship with nature and the Earth, to achieve a fair balance between the economic, social and environmental needs of present and future generations"*[19].

The *right of future generations to a clean, healthy environment* is also stipulated in another international document, such as *"Agenda 2030"*, adopted by the UN General Assembly through the resolution on 25 September 2015, no. 70/1, entitled *"Transforming Our World: the 2030 Agenda for Sustainable Development"* (A/RES/70/1), distributed on 21 October 2015[20]. The signatory states engaged to transmit ***to future generations goods and rights that have to be ensured and guaranteed in relation to the relationship between military technologies and their employment in order to manipulate the environment or hostile ones that broadly affect or could affect the environment in a severe manner.*** Such rights are: the right of individuals, peoples, the society in its aggregate to a *clean and healthy global environment*; the right of individual, of peoples, *to an international climate of peace and security*; the right of individual, of peoples to live on *a clean, secure and resource-rich planet*; the right of individual, of peoples *to live a life free from fear, terror, misery and indecency caused by poverty and human rights violations*.

[17] *Johannesburg Declaration on Sustainable Development*, 4 September 2002, https://ec.europa.eu/environment/archives/wssd/documents/wssd_pol_declaration.pdf, retrieved on 7 September 2016.
[18] *Chronology of Harmony with Nature*, www.harmonywithnatureun.org/chronology.html, retrieved on 7 September 2016.
[19] *Ibidem*.
[20] See https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf, retrieved on 7 September 2016.

ROMANIAN MILITARY THINKING

Through the document entitled *"Agenda 2030"*, the right of future generations related to the environment is expressly stipulated. They benefit from: the right *to development*; the right *to a future global environment characterised by peace and security*; the right to live in a *future world free from worry, fear, misery and needs*; the right to live in a future world *free from poverty;* the right *to enjoy a clean, unpolluted and resource-rich environment*; the right *to live on a safe and clean planet*.

Expressly, the Preamble of "Agenda 2030" stipulates the obligation of the states parties to respect and pursue in their policies and in multilateral or bilateral cooperation certain goals that are directly linked to the relationship environment-armed conflicts. Among them, we mention "peace dimension" (entailing the establishment of societies that are tolerant, inclusive, peaceful and just, free from violence and fear; the connection between sustainable development and peace).

Expressly, the Preamble of *"Agenda 2030"* stipulates the obligation of the states parties to respect and pursue in their policies and in multilateral or bilateral cooperation *certain goals that are directly linked to the relationship environment-armed conflicts.* Among them, we mention *"peace dimension"* (entailing the establishment of societies that are tolerant, inclusive, peaceful and just, free from violence and fear; the connection between sustainable development and peace).

Point 14 in the Agenda is linked to the issues of underdevelopment, natural disasters, *threats to global security, conflicts, violent extremism, terrorism and humanitarian crises or forced movement of people*. *"Agenda 2030"* obliges states parties to take action in order to: ***resolve and prevent conflicts, sustain post-conflict reconstruction of countries***, as well as to ensure that women are really involved in the ***processes of peace construction and state creation.*** States parties have also the obligation to comply with international law, in the sense of respecting the right of peoples to development and to self-determination.

We consider that, with regard to the legal content of some future international conventions subsequent to *"Agenda 2030"*, it should:

- provide for strengthened legal obligations of states *regarding the preservation of peace and international security*. This obligation should be accompanied by *clear responsibilities* (according to the principle in the environmental law

With regard to the relationship between the environment and the obligation of states to use it in a peaceful, non-destructive way, not to subject it to degradation or irremediable destruction following a military action, we can also mention the principles established by the Rio Declaration, adopted following the Rio Summit (Earth Summit): the right of all peoples to a healthy, productive life in harmony with nature; the sovereign right of nations to freely exploit their own resources without thereby causing cross-border damage to the environment; the polluter pays principle; the obligation of nations to adopt effective laws on the environment etc.

"the polluter pays" and where the use of military or civilian technologies for military or hostile purposes, which have caused or are susceptible of causing a negative, severe, and long-term impact on the environment or to irremediably destroy it, *to be considered as "destructive action on the environment"*, involving obligations for the actor to repair the harm as well as other concrete actions to restore the ecosystems affected by the armed aggressions, through the destructive impact on the environment);

- *the states that conduct armed actions to destroy and attack other nations* should be subject to a strengthened legal system regarding the responsibility for the environmental destruction following their aggressive armed actions or having a military component.

With regard to the relationship between the environment and the obligation of states to use it in a peaceful, non-destructive way, not to subject it to degradation or irremediable destruction following a military action, we can also mention the principles established by the Rio Declaration[21], adopted following the Rio Summit on 3-12 June 1992, also named Earth Summit: the right of all peoples to a healthy, productive life in harmony with nature; the sovereign right of nations to freely exploit their own resources *without thereby causing cross-border damage to the environment;* the polluter pays principle; the obligation of nations to adopt effective laws on the environment etc.*[22].* According to Principle 24 in the Rio Declaration, it is considered that *war intrinsically exercises a destructive action on sustainable development*, therefore the express obligation of states to conform to the international law norms regarding environmental protection during armed conflicts and to participate in the development of this law, if necessary[23].

Practically, this principle legally characterises the *environment as a "civilian good",* states having to renounce attacking and affecting/destroying the environment in the event of an armed conflict or attack on a military objective, if the damage caused or susceptible

[21] See https://www.cbd.int/doc/ref/rio-declaration.shtml, retrieved on 7 September 2016.
[22] Daniela Marinescu, *op. cit.*, pp. 18-19.
[23] *Ibidem*, p. 601.

of being caused to the environment would be greater than those to the target objective[24]. The Doctrine mentions, in this context, the UNGA Resolution AG ONU 43/37, on 9 February 1993, entitled *Protection of the Environment in Times of Armed Conflict*[25]. In this resolution, the UNGA considers the the unjustified destruction of the environment in relation to military needs as well as that of a gratuitous nature are clearly contrary to the international law in force (paragraph 32). The approval of the International Court of Justice (requested by the UNGA through resolution 49/75 K in 1994), which cites this resolution in its jurisprudence, with regard to the relationship between the environment and armed conflicts, implicitly considers as having an *illegal character the threat or use of nuclear weapons* (that cause severe, long-term or irreparable damage to the environment).

Another important international document is also the *Millennium Declaration*, adopted following the World Summit in 2000[26], a document in which, in points 4 and 6, it is also mentioned the *objective of protecting and preserving the environment* (expressed by the *value of respect for nature*). However, this is an objective that should be *correlated with the other principles and objectives* of the Declaration, among which there are some that have a direct relevance for the present topic: ***preservation of a climate of peace and international security***; the right to development; ***protection of vulnerable groups (including those who have suffered as a result of genocide, civil wars, natural disasters);*** improvement of cooperation relations between countries[27]. Point 6 in the Millennium Declaration *(respect for nature)* sanctions the principle of the need to transmit to future generations the rich resources of the planet, including through the *introduction*

In Millennium Declaration, adopted following the World Summit in 2000, a document in which, in points 4 and 6, it is also mentioned the objective of protecting and preserving the environment (expressed by the value of respect for nature).

[24] *Ibidem*, p. 602.
[25] *Ibidem*. See also A RES 43/97 *Protection of the Environment in Times of Armed Conflict*, on 9 February 1993, https://undocs.org/en/A/RES/47/37, retrieved on 12 February 2020. See also A RES 37/137/*Protection against Products Harmful to Health and to Environment*, 17 December 1982, https://undocs.org/en/A/RES/37/137, retrieved on 12 February 2020; A RES 47/195, 1 March1993, *Protection of Global Climate for Present and Future Generations of Mankind*, https://undocs.org/en/A/RES/47/195, retrieved on 12 February 2020.
[26] UNGA, Resolution 55/2, *United Nations Millennium Declaration*, New York, 8 September 2000, www.un.org/millennium/declaration/ares552e.htm, retrieved on 12 February 2020.
[27] Paul Boncuțiu, *Declarația Mileniului*, Part one, year 2000, 12 December 2010, Ziare.com, http://www.ziare.com/international/onu/declaratia-mileniului-partea-intai-anul-2000-1061123, retrieved on 12 February 2020.

of the principle of moderation in the management of all living species and natural resources[28].

The UN Secretary-General, Ban Ki-Moon, considered, in 2015[29], that one of the global challenges to the society in the 21st century is represented by the ***climate changes, to which are added challenges to peace and international security*** *and to human rights*. It is the obligation of states to create a *universal climate of peace and international security*, connected to the *need to protect the environment (**war being another cause of the sometimes-irreversible degradation and pollution of nature)***, he considered. In his vision, the problem of climate change should be seen as connected to *"the global problems – financial, economic, internal, **security**, influencing food security, health and water"*[30].

The UN Secretary-General, Ban Ki-Moon, considered, in 2015, that one of the global challenges to the society in the 21st century is represented by the climate changes, to which are added challenges to peace and international security and to human rights.

Climate changes are seen by Ban Ki-Moon, in another speech, *as entailing **"all nations in the world legal obligation as well as interest to preserve a universal climate of peace and security"***[31]. **Climate changes** represent, in his view, *"a multiplier of threats, especially at international level, extreme weather and natural disasters caused by them leading to humanitarian crises and increasingly massive displacements of population to rich countries, endangering international security"*[32].

At European level, it can be noted the *EU interest in contributing to not only the efforts to consolidate the environment international law but also to a strengthened legal protection related to the environment*, in response to France initiative to negotiate a so-called *Global Pact for the Environment*[33] at international level. The initiative is meant to ease the implementation of already existing international environmental law. The project was introduced to the UNGA by France,

[28] UNGA, Resolution 55/2, *loc. cit.*

[29] Secretary-General Ban Ki-Moon, Paris, 29 April 2015, *Address at the Institute d'Etudes Politiques de Paris: The United Nations at 70: New Global Challenges: A Conversation with Ban Ki-Moon*, UN News Centre, www.un.org/apps/news/infocus/sgspeeches, retrieved on 12 February 2020.

[30] *Ibidem*.

[31] *Declaration – Secretary-General's Message to High-Level Side Event on Climate Change and Security* (delivered by Janos Pasztor), New York, 30 September 2015, www.un.org/sg/statements, retrieved on 12 February 2020.

[32] *Ibidem.*

[33] *European Commission Roadmap*, Ref. Ares (2018)900428 - 15/02/2018, http://pactenvironment.org, retrieved on 12 February 2020.

on 19 September 2017, following the UNGA 72nd session ministerial meeting[34]. At the proposal of France, it was noted the idea of establishing a *Group of Friends of the Pact*, to issue a draft of a resolution to be adopted by the UNGA and formally open the debates for this Pact (with topics on the negotiating table in 2018)[35]. The purpose of the Group of Friends of the Pact is to establish a working group open to negotiate the Pact under the auspices of the UNGA, expected to complete its work this year, when it is desirable to present the outcome of an intergovernmental conference. In this context, it is considered that the EU has competence in the field provided by art. 192 (1) TFEU (environmental protection). The Commission can act only on the basis of the authorisation issued by the Council to negotiate this international instrument on behalf of the EU[36].

It is important to note that the *Global Pact for the Environment* proposed by France is intended to be, from the very beginning, a *codification of the principles included in the Rio Declaration, as the third international pact.* It is included in the category of international pacts related to human rights, as the International Pact on Civilian and Political Rights /1966, the International Pact on Economic, Cultural and Social Rights /1966 or even the Universal Declaration of Human Rights in 1949. On 10 May 2018, the UNGA adopted Resolution 72/277, entitled *"Towards a Global Pact for the Environment"*[37].

In the *Global Pact for the Environment*, subject to the discussions within the UNGA, following the French initiative, since 2017, there are *important innovations and codifications*, such as: establishing a universal right to a healthy, intact environment as a human right that can be invoked before the courts at national, international and regional level; unifying the guiding principles of international environmental law into a single legal document; empowering citizens to hold their and neighboring governments accountable for environmental policies[38].

ROMANIAN MILITARY THINKING

In the Global Pact for the Environment, subject to the discussions within the UNGA, following the French initiative, since 2017, there are important innovations and codifications, such as: establishing a universal right to a healthy, intact environment as a human right that can be invoked before the courts at national, international and regional level; unifying the guiding principles of international environmental law into a single legal document; empowering citizens to hold their and neighboring governments accountable for environmental policies.

[34] *Ibidem.*

[35] *Ibidem.*

[36] *Ibidem.*

[37] *Global Pact for the Environment*, https://www.iucn.org/commissions/world-commission-environmental-law/wcel-resources/global-pact-environment, retrieved on 12 February 2020.

[38] *Ibidem.*

At European level, within the EU, it is to note the recent document entitled *European Green Pact*[39], which is intended to be a priority of the European Commission, led by Ursula von der Leyen. Through this Pact, a real European government programme proposed and assumed by the European Commission in 2020, it is acknowledged by the EU that *"the climate change and the global climate are significant threat multipliers and a source of instability"*. *The security interests*, mentioned in this context, *"are factors that will be changed by the ecological transition"*[40], a fact that, in the EU view, will create challenges for a certain number of countries and societies. The EU will launch the *European Pact on Climate* in March 2020, to encourage the extended understanding (at the public opinion level) of environmental threats like *security threats* as well as the way to combat such threats[41]. It is important to mention the EU commitment through the European Commission, which launched that ambitious Pact, to encourage the *"cooperation with all partners" (states, non-state actors, third party states, member states) to "increase the capacity to prevent environment threats from becoming sources of conflict, global insecurity, population displacement and forced migration"*[42]. According to the Commission, the EU foreign policy and the common defence and security policy should include the climate policy dimension[43]. However, the impact of military or civilian technologies used for military or other hostile purposes on the environment, and the measures to prevent the degradation or destruction of the environment as a direct result of wars and armed conflicts of any type are not included in the document.

European Green Pact is intended to be a priority of the European Commission, led by Ursula von der Leyen. Through this Pact, a real European government programme proposed and assumed by the European Commission in 2020, it is acknowledged by the EU that "the climate change and the global climate are significant threat multipliers and a source of instability".

CONCLUSIONS

As it can be seen, this is an area of international environmental law exploring a legal relationship (environment – armed conflict) that we consider of great importance for the society of the 21st century,

[39] Brussels, 11.12.2019 COM (2019) 640 final. *Communication from the Commission to the European Parliament, European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Green Deal*, https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_en.pdf, retrieved on 12 February 2020.
[40] *Ibidem*.
[41] *Ibidem*.
[42] *Ibidem*.
[43] *Ibidem*.

given the constant technological and scientific advance in military and civilian technologies, but used for hostile purposes, as well as the arms race, which we are currently witnessing, as a resumption of the neo-realistic perspective in international politics. The *environment and international environmental law are becoming, both from the perspective of global issues such as climate change and those set out here, key areas* for providing increased protection for terrestrial ecosystems and their parts that can be exposed or are actually exposed, in the event of crises with a military component or of military conflicts, including regional ones, to the danger of long-term, serious or irreparable destruction or degradation.

It is important that the relevant international doctrine and jurisprudence *acknowledge the need for the express sanctioning, at the level of an international convention on this subject, of the environment as a civil good.* They should also include the *express prohibition* on states, but also on non-state actors involved in armed conflicts, to use the environment for military purposes, the environment as a military component of the particular war or conflict. An express *ban on the use of weapons of mass destruction on the environment*, either for no specific purpose, for the purpose of intimidating other states or for the purpose of aggression against other states or groups of states, should also be introduced. The *ban on the use of drones in military conflicts in order to destroy the environment under the jurisdiction of other states or in free zones* should also be introduced. The ban on the use of civil technologies for environmentally hostile purposes should also be introduced, whether we are talking about a mixed or urban natural environment (artificial, i.e. human settlements). Legal correlations and improvements can be made between the classic conventions already adopted by states on the conduct of wars and the recent obligations assumed by states through the Rio, Johannesburg or *"Agenda 2030"* declarations.

It results that we are in the presence of an *area that needs to be legally improved*, both through the efforts of states (through the debate and adoption *by the UN General Assembly of various resolutions* or by *signing an international convention* specifically dedicated to this subject) and through the *involvement of non-governmental actors* (NGOs, global media, organisations, transnational corporations)

ROMANIAN MILITARY THINKING

The environment and international environmental law are becoming key areas for providing increased protection for terrestrial ecosystems and their parts that can be exposed or are actually exposed, in the event of crises with a military component or of military conflicts, including regional ones, to the danger of long-term, serious or irreparable destruction or degradation.

to preserve the environment and transmit it to future generations as a healthy, clean environment, unaffected by the destruction caused by wars and armed conflicts or by civilian technologies used for environmentally hostile purposes.

BIBLIOGRAPHY:

1. ***, A RES 37/137/*Protection against Products Harmful to Health and to Environment*, 17 December 1982. https://undocs.org/en/A/RES/37/137.
2. ***, A RES 47/195, 1 March 1993, *Protection of Global Climate for Present and Future Generations of Mankind*, https://undocs.org/en/A/RES/47/195.
3. ***, A RES 43/97 *Protection of the Environment in Times of Armed Conflict*, 9 February 1993. https://undocs.org/en/A/RES/47/37.
4. ***, *Global Pact for the Environment*, https://www.iucn.org/commissions/world-commission-environmental-law/wcel-resources/global-pact-environment.
5. ***, *Harmony with Nature*, Report of the Secretary General, UNGA, A/67/317.
6. ***, *The Millennium Development Goals Report*, 2014, *We Can End Poverty*, United Nations, New York, 2014, www.undp.org/content/undp/en.
7. ***, Resolution adopted by the General Assembly, 60/192, *International Year of Planet Earth*, 2008, A/RES/60/192.
8. ***, Secretary-General Ban Ki-Moon, Paris, 29 April 2015, *Address at the Institute d'Etudes Politiques de Paris: The United Nations at 70: New Global Challenges: A Conversation with Ban Ki-Moon,* UN News Centre, www.un.org/apps/news/infocus/sgspeeches.
9. ***, UNGA, Resolution 55/2, *United Nations Millennium Declaration*, New York, 8 September 2000, www.un.org/millennium/declaration/ares552e.htm.
10. Paul Boncuțiu, *Declarația Mileniului*, Part one, year 2000, 12 December 2010, Ziare.com, http://www.ziare.com/international/onu/declaratia-mileniului-partea-intai-anul-2000-1061123.
11. Daniela Marinescu, *Tratat de dreptul mediului*, IVth edition, updated and supplemented, Editura Universul Juridic, București, 2010.
12. Adrian Năstase, *Documenta universales I, Documente fundamentale ale dreptului internațional contemporan și ale relațiilor internaționale,* Roxana Frailich (ed.), Asociația Română pentru Educație Democratică, Regia Autonomă Monitorul Oficial, București, 1997.

WEBOGRAPHY:

1. http://www.un.org/en/events/motherearthday/documents.shtml
2. https://www.un.org/en/universal-declaration-human-rights/

3. https://www.cbd.int/doc/ref/rio-declaration.shtml
4. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf
5. https://ec.europa.eu/environment/archives/wssd/documents/wssd_pol_declaration.pdf
6. file:///C:/1976-enmod-icrc-factsheet.pdf
7. https://www.unog.ch/enmod
8. https://www.refworld.org/docid/3b00f22a10.html.

ON ROMANIA CROSS-BORDER COOPERATION EUROREGIONS

Senior Lecturer Vasile BOGDAN, PhD
DANUBIUS University, Galaţi

Viorel-Cătălin MIHALCEA, PhD Candidate
"Carol I" National Defence University, Bucharest

Populations of different ethnicities have to live in different states, separated by borders that mutilate the national feeling and the perspective of the populations. In the relatively recent period, the European Union has proceeded to overcome the sequelae of the past, switching to creating bridges between neighbouring states, which have populations living on both sides of the border. The approach serves the need for balance, peace and detente in areas that have been difficult for conflict in the past. The initiative came from the West, mainly due to German concerns, the space being severely tested during the last world conflagrations. In the established cross-border collaborations, the most important is the economic-financial support for raising the standard of living and expectation in the poor communities. In this context, regarding the cross-border collaboration in the area bordering the national territory, Romania presents itself as extremely constructive, being part of 12 Euroregions, across all the borders of the country.

Keywords: territorial cooperation, macro-regions, standard of living, regional development, stability pillars.

INTRODUCTION

It is in the logic of history that the great powers at a particular time conduct destabilising actions resulting in stopping the unitary development of the nations in terms of affirmation and habitation. Obviously, it is the case of the Romanian people, severely tested, throughout history, as far as the collective being is concerned, because of territorial losses. Thus, the descendants of the Romanians were forced to live in areas in the composition of different states either neighbouring Romania or even remote ones.

In such conditions, the discontinuity, spatial and political, produced in the survival of the Romanian people in the same body, should constitute the strategic impetus in the efforts to overcome the temporary borders that separate isolated spaces, of the utmost importance being the desire for collaboration and support of the ethnic nuclei from outside the country. As it is known, territories of Romania started to be annexed by other countries in 1940, from all four cardinal directions, Romania drastically reducing its surface, resources and population.

GENERAL CONTEXT

The European Union consists of 27 states that are closely linked, thus ensuring the flow of labour force, capital, goods and services. As a protection measure against the wave of globalisation, different ways of counteracting it can be activated. Structures of the same ethnicity, separated in the historical past, can now exist in the composition of different states, thus separated by national borders. It is the merit of the European Union to have created the legal framework necessary for multiple cooperation and support, achieved between the ethnic groups divided by the current borders. Maintaining subordination to the national responsible bodies, the structures in the territories are provided with the opportunity to identify solutions for local administration through their own efforts, to achieve the standard

The European Union consists of 27 states that are closely linked, thus ensuring the flow of labour force, capital, goods and services. As a protection measure against the wave of globalisation, different ways of counteracting it can be activated. Structures of the same ethnicity, separated in the historical past, can now exist in the composition of different states, thus separated by national borders.

of living with the perspective of future progress, in relation to the possibilities available to them in the territory.

The fundamental legal documents related to cross-border cooperation are represented by the *Treaty of Maastricht* (signed on 7 February 1992 and entered into force on 1 November 1993), the *Treaty of Rome* (signed on 25 March 1957, taking effects after 1 January 1958), the *Treaty of Lisbon* (signed on 13 December 2007, entered into force on 1 December 2009), as well as the *decisions* and *accession treaties*[1]. Regional as well as local development is desirable to provide regional and local communities with funds and facilities, to materialise some initiatives at the local level, to provide solutions to some social needs and to foster the welfare of the communities in the territory[2]. In this regard, after 2004, a *law on regional development* was adopted in Romania[3].

Euroregions appeared beginning 1990 in Western Europe, after the fall of the Iron Curtain, following the line of former separation, near the borders of Germany, France, the Netherlands, Belgium, and Switzerland. Likewise, (following the German example) Euroregions appeared at the point of contact between Western and Central Europe (Germany, Poland, Czechia) and Eastern Europe (Russia, Latvia, Poland).

Territorial cooperation is intended to agree on, to launch and conduct unitary actions, subsumed under the policies of unitary development of territories that are, administratively, under separate jurisdictions[4]. In the regional development paradigm, we will consider *Euroregions* as *"... areas or regions of economic and not only interference between two or more states that, in common, capitalise on the material and human resources by initiating activities and programmes in agriculture, industry, transportation, telecommunications, tourism, commerce"*[5]. Euroregions appeared beginning 1990 in Western Europe, after the fall of the *Iron Curtain*, following the line of former separation, near the borders of Germany, France, the Netherlands, Belgium, and Switzerland. Likewise, (following the German example) Euroregions appeared at the point of contact between Western and Central Europe (Germany, Poland, Czechia) and Eastern Europe (Russia, Latvia, Poland).

1 Romanian Academy, Institute of Geography, Radu Săgeată (coord.), *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării (Cross-border Cooperation Euro-Regions in the Lower Danube Basin)*. Geographical Study, Editura Academiei Române, București, 2014. Table 10. System of Euroregions on the eastern border of Romania, pp. 29-32.

2 Tiberiu Brăilean, *Dezvoltare regională și cooperare transfrontalieră*, Editura Junimea, Iași, 2007, p. 21.

3 *Law no. 315 on 28 June 2004 (updated) on Regional Development in Romania*, published in the *Official Gazette* no. 577 on 29 June 2004.

4 Adrian Pop (coord.), Dan Manoleli, *Spre o strategie europeană în bazinul Mării Negre. Cooperarea teritorială,* Institutul European din România, București, 2008, p. 53.

5 *Stadiul actual al reglementărilor naționale și comunitare în domeniul cooperării transfrontaliere*, Editura Primus, Oradea, 2009, p. 43.

After 2007, Euroregions were created in Eastern Europe (Carpathian area[6], the Lower Danube, the Danube-Mureș-Tisa or the Upper Prut)[7].

Cross-border cooperation is robust in the Baltic region, as a consequence of the involvement of the states having a consolidated democracy and a high economic and social development level; therefore, we can state that there is an opportunity for the inhabitants to acquire a proper standard of living. Between international actors there have been signed bilateral or multilateral agreements to support partnership initiatives[8]. The successive stages of cross-border relations can be as follows: exceeding border limits and manifesting relations between entities and populations, exchanging information, especially between local authorities, unanimous acceptance, cooperation, optimisation and integration of regional development programmes[9]. The latter two stages have not been achieved yet, representing only hypotheses related to future cooperation possibilities[10].

THE SYSTEM OF EUROREGIONS IN THE PROXIMITY OF ROMANIA

In the proximity of Romania, history has been generous in terms of creating certain areas having ethnic continuity and being under the jurisdiction of many states. It is important to know that cross-border cooperation regions have preserved the defining features of the ethnic element and the good relations between neighbours as well as the mutual cooperation with the motherland. It should also be mentioned that the arbitrary borders have hampered the natural transfer of influences, nevertheless, without interruptions in the flows of collaboration.

In the proximity of Romania, history has been generous in terms of creating certain areas having ethnic continuity and being under the jurisdiction of many states. It is important to know that cross-border cooperation regions have preserved the defining features of the ethnic element and the good relations between neighbours as well as the mutual cooperation with the motherland.

The storms of history have placed Romanian populations in all cardinal directions, in relation to Romania. The cross-border cooperation produced with the intention of beneficially meeting the desires of mutual knowledge, of joint effort, more sustained development, with the attainment of better levels of common welfare, all of them found

6 Poland, Slovakia, Hungary, Ukraine and Romania.

7 Vasile Bogdan, *Euroregiuni de cooperare transfrontalieră ale României*, Editura CTEA, București, 2019, pp. 31-33.

8 European Union, *Practical Guide to Cross-Border Cooperation. Euro Dobrogea*, Constanța, 2005, pp. 25-26.

9 ***, Council of Europe, *Cross-Border Cooperation Manual*, București, 2000, p. 56.

10 Vasile Bogdan, *op. cit.*, pp. 45-48.

the right understanding, with the acceptance of the limits of the local implications. It is noteworthy that Romania is part of the establishment of the Euroregions towards all the cardinal directions:

- on the eastern border, there are the *Lower Danube*, the *Siret-Prut-Dniester* and the *Upper Prut* Euroregions;
- on the western border, we highlight the *Bihor-Hajdú-Bihar,* the *Danube-Criş-Mureş-Tisa*, as well as the *Middle Danube-Iron Gates* Euroregions;
- on the northern border, there is the *Carpathian Euroregion*, comprising the territory belonging to five states (Poland, Slovakia, Hungary, Ukraine and Romania);
- on the southern border, there are the *"Danube 21" Cross-Border Cooperation Association* and the *Southern Danube, Giurgiu-Ruse, Danubius* and the *Danube- Dobruja* Euroregions[11].

The Euroregions on the state borders of Romania should be also analysed as part of the Danube micro-region, being situated on the Rhin-Main-Danube axis or in the Pontus Euxinus area. The analysis of the Danube macro-region should be conducted in a manner that is similar to the Adriatic and Ionian, Alps or Baltic Sea macro-regions *(figure no. 1)*[12].

Figure no. 1: the Danube macro-region[13]

[11] *Ibidem*, pp. 103-175.
[12] According to http://www.interreg-danube.eu/, retrieved on 13.12.2019.
[13] Source: http://www.danube-region.eu/, retrieved on 13.12.2019.

The stability pillars will be ensured by: strengthening the potential of the Danube macro-region, connecting the region to similar identities, in the context of water transport, the existence of the possibilities of terrestrial, air and railway systems, the protection of the environment (with diminishing the natural and anthropic risks, increasing the quality of water, soil, air and biodiversity), building welfare and prosperity (through competitiveness, population involvement, specialisation and multidisciplinary training), all these aspects being subsumed under the requirements of the knowledge society[14].

THE EUROREGIONS ON THE EASTERN BORDER

In a progressive manner, on the eastern border of Romania, following 1997, three Euroregions have been defined: *the Lower Danube, the Upper Prut and the Siret-Prut-Dniester*. Indisputably, the Euroregions are placed in the framework of outer European Union and NATO borders, generating particular aspects regarding their geopolitical integration[15] *(table no. 1)*.

Euroregion generic data	Countries involved
The Lower Danube Established in 1997-1998 Area 53,496 km²	Romania
	Ukraine
	Republic of Moldova
The Upper Prut Established in 2000 Area 42,809 km²	Romania
	Ukraine
	Republic of Moldova
The Siret-Prut-Dniester Established in 2002 Area 31,434 km²	Romania
	Republic of Moldova

Table no. 1: Euroregions situated on the eastern border of Romania[16]

The priorities of the Euroregions on the Romanian eastern border are related to the following major objectives: to develop a more competitive economy in the cross-border area, to ease the pressure on the environment and to prepare for the expansion of the "*people to people"* type of manifestation (extended cooperation between

[14] *Ibidem.*
[15] Vasile Bogdan, Emanuel-Ştefan Marinescu, *Cooperarea transfrontalieră şi studii de arie. Curs*, Editura CTEA, Bucureşti, 2019, pp. 35-36.
[16] Romanian Academy, Institute of Geography, *op. cit.*, p. 61.

ROMANIAN MILITARY THINKING

The stability pillars will be ensured by: strengthening the potential of the Danube macro-region, connecting the region to similar identities, in the context of water transport, the existence of the possibilities of terrestrial, air and railway systems, the protection of the environment (with diminishing the natural and anthropic risks, increasing the quality of water, soil, air and biodiversity), building welfare and prosperity (through competitiveness, population involvement, specialisation and multidisciplinary training), all these aspects being subsumed under the requirements of the knowledge society.

the communities within the cross-border area)[17]. In the Prut adjacent space, the two metropolitan areas are revealed, Iaşi and Brăila-Galaţi.

The *Lower Danube* was established following Romania's attempts to form the Euroregion, made at the Ismail Summit, on 3-4 July 1997. The *"Declaration on Cross-Border Cooperation"* was signed by the Presidents of Romania, Ukraine and the Republic of Moldova[18]. On 14 August 1998, in Galaţi, it was signed the *"Agreement on Establishing the Lower Danube Euroregion"*. After the events in 2014-2015, between Ukraine and the Russian Federation, the territorial delineation in the Crimean Peninsula changed radically *(figure no. 2)*.

Figure no. 2: the Lower Danube Euroregion[19]

[17] Cosmin Sabău, *Efectele benefice ale cooperării transfrontaliere în euroregiuni: Euroregiunea Bihor-Hajdú-Bihar*, Editura Mirton, Timişoara, 2012, pp. 148-149.

[18] Romanian Centre for European Policies, *Contribution to the Partnership for Development between Romania and the Republic of Moldova*, 29 May 2013, Chişinău, p. 14.

[19] Radu Săgeată (coord.), *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, Editura Academiei Române, Bucureşti, 2014, figure no. 29, p. 66.

The *Siret-Prut-Dniester* Euroregion was established by signing the *"Protocol on the Cross-Border Cooperation in the Siret-Prut-Dniester Euroregion"*, on 18 September 2002, in Iaşi, following the initiatives of the Local Councils in Romania and the Republic of Moldova[20]. On 4 December 2002, in Ungheni (the Republic of Moldova), it was signed the *Statute on the Functioning of the Siret-Prut-Dniester Euroregion*, at the Forum of Presidents[21] *(figure no. 3)*.

Figure no. 3: the Siret-Prut-Dniester Euroregion[22]

The organisational aspects were set at the *Forum of Presidents*, a meeting that took place in Ialoveni (the Republic of Moldova), on 6 April 2004. On that occasion, it was approved the *"Regulation on the Organisation and Functioning of the Siret-Prut-Dniester Euroregion"*, the document having some significant modifications. The three Romanian counties are territorial entities having a different economic potential, the value of Iaşi County being indisputable, considering the city was the capital of former province Moldova.

[20] Ion Talabă, *România şi tematica euroregiunilor*, in *Euroregiunile. Prezent şi viitor*, Editura Performantica, Iaşi, 2005, p. 198.

[21] Felicia Dediu, *Participarea României la realizarea unor iniţiative în domeniul cooperării tranfrontaliere regionale*, in *"Carol I"* NDU Bulletin, no. 4/2007, pp. 221-222.

[22] See *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic* (Radu Săgeată coord.), *loc. cit.*, figure no. 22, p. 78 (1.- Capital. 2. – Polarisation nucleus. 3. – Cross-border connections. 4 - Airports. 5 - Borders. 6 – Administrative limits).

The *Upper Prut* Euroregion was established following the Romanian initiative, the beginning being marked by the *"Treaty on Good Neighbourhood and Collaboration Relations between Romania and Ukraine"* signed on 2 July 1997[23]. It should be also mentioned the *"Agreement on the Establishment of the Upper Prut Euroregion"*, a document signed on 22 September 2000, in Botoşani *(figure no. 4).*

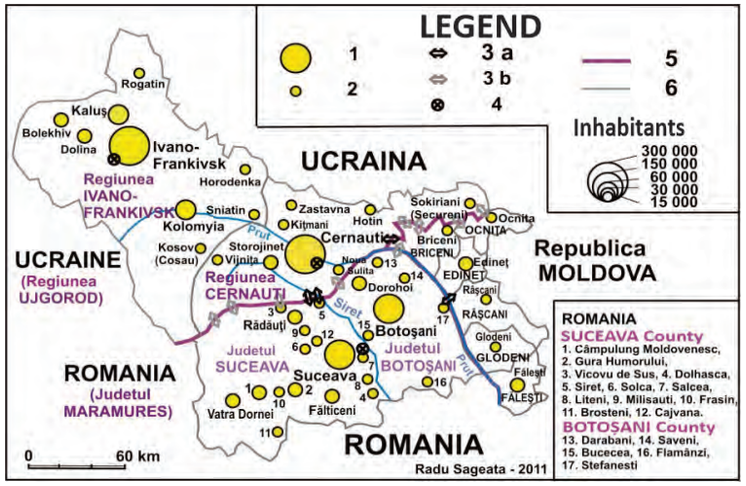

Figure no. 4: the Upper Prut Euroregion[24]

The Upper Prut Euroregion was established following the Romanian initiative, the beginning being marked by the "Treaty on Good Neighbourhood and Collaboration Relations between Romania and Ukraine" signed on 2 July 1997.

The leadership is ensured by a Council, and the functions are exercised through the Presidency and the Secretariat of the Euroregion Council as well as through the Coordination Centres (in Bălţi, Suceava and Cernăuţi) and four working commissions[25]. The four working commissions have complementary priorities: commission 1 (economy, infrastructure and tourism), commission 2 (ecological security, environment protection and bioeconomy), commission 3 (collaboration in the field of science, education, culture, healthcare, sports and youth) and commission 4 (enhancement and harmonisation of inter-regional, inter-ethnic relations and local leadership)[26].

[23] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 116-118.
[24] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, loc. cit., figure no. 28, p. 87 (1.- Regional polarisation nuclei. 2.- Local polarisation nuclei. 3. – Cross-border connections: 3 a. International traffic. b. Small border traffic. 4 - Airports. 5 - Borders. 6 – Administrative limits).
[25] Andrei Balînschi, *Problemele şi perspectivele dezvoltării Eurorehiunii "Prutul de Sus" în condiţiile proceselor integrării europene*, în *Euroregiunile. Prezent şi viitor*, *op. cit.*, p. 201.
[26] Felicia Dediu, *op. cit.*, p. 220.

It should be noted the intention of local communities to create a space of collaboration, mutual aid and progress of the mentioned cross-border areas, taking into account the Russian Federation geostrategic implications. In this regard, it is necessary to be aware of the control and influence measures that come from the outside, present eastward of the Romanian border, which limit the collaboration efforts and affect the population resilience. The major deficit in financial resources makes necessary a massive financial support. It is certain a slow economic development, population aging, pauperisation and decrease in number, as well as the modest level of road communications, the poor promotion of tourism, the industrial and transport (road and rail), park reduced and outdated, the mediocre level of education, the massive migration of local work force to the East and the West. In this regard, measures are needed to protect the environment, in order to stop the degradation of the standard of living in the rural sector, which is at the level of extreme poverty, as well as energetic measures for accessing European funds[27].

THE EUROREGIONS ON THE NORTHERN BORDER

The northern border of Romania, situated in the context of the European Union and NATO external border, is on the Baltic-Pontic axis, well known for the political pressures at the regional level.

The *Carpathian Euroregion* comprises five states: Hungary (5 counties), Poland (4 voivodeships), Slovakia (9 counties), Ukraine (4 regions) and Romania (7 counties)[28]. The included counties in Romania are Satu Mare, Maramureş, Sălaj, Bihor, Suceava, Botoşani and Harghita (starting in 2000). The Euroregion was established on 14 February 1993, in Debrecen (Hungary), on the occasion of the meeting of the foreign ministers of the interested countries, in which the local administration representatives were present[29] *(figure no. 5)*.

The constitutive documents are the *"Agreement on the Establishment of an Inter-Regional Association the ‹Carpathian Euroregion›"* and the *"Statute of the Inter-Regional Association the ‹Carpathian Euroregion›".* Its management is ensured by the Carpathian Euroregion Council, the decision-making body in terms of the Euroregion strategy

[27] Vasile Bogdan, *op. cit.*, pp. 93-94.
[28] Ion Talabă, *op. cit.*, p. 193.
[29] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 134-143.

and the problems of major interest. The international Secretariat was initially based in Uzgorod (Ukraine), being then moved in Debrecen (Hungary). The working commissions are under the responsibility of a state as follows: Regional Development (Hungary), Prevention of Natural Disasters (Slovakia), Tourism and Environment (Poland), Trade Development (Romania) and Social Infrastructure (Ukraine)[30].

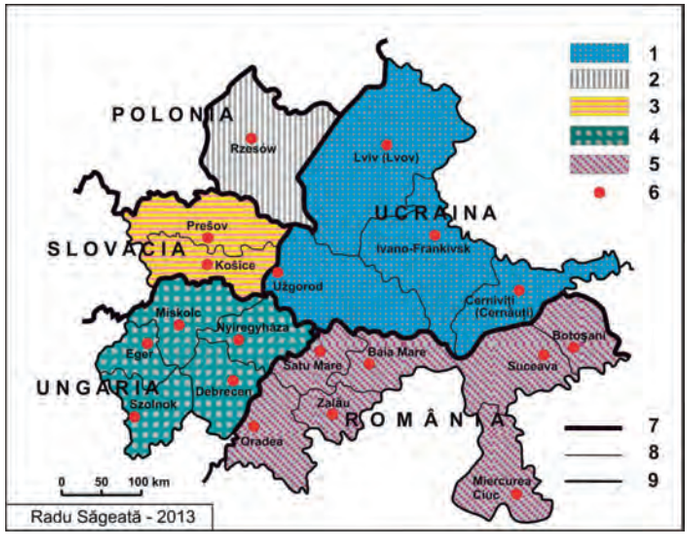

Figure no. 5: the Carpathian Euroregion[31]

The Carpathian Euroregion is a unique cross-border structure as there are bi- and trilateral contacts. In the existence of the Euroregion, it is important the message transmitted to the peoples of Europe, namely that such cooperation could be feasible. Moreover, it is an impetus for other Euroregions in Europe to work and develop, in terms of cooperation, dialogue and mutual aid.

The *Carpathian Euroregion* is a unique cross-border structure as there are bi- and trilateral contacts. In the existence of the Euroregion, it is important the message transmitted to the peoples of Europe, namely that such cooperation could be feasible. Moreover, it is an impetus for other Euroregions in Europe to work and develop, in terms of cooperation, dialogue and mutual aid. It is validated the symbolism of establishing an Euroregion having four members, as a space for collaboration and progress, to demonstrate the viability of the European Union in the field of regional development and cross-border cooperation with multiple participation. It is noted the sense of entrepreneurship and the diversified practices, as well as

[30] Cristina Dogot, *Romanian Local Administrations and Their Activities in Carpathian Euroregion*, in *Cross-Border Cooperation. Models of Good Practice in the Carpathian Region* (Adrian-Claudiu Popoviciu, editor), Editura CH Beck, Oradea, 2014, pp. 174-175.

[31] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, *loc. cit.*, figure no. 52, p. 128 (1-5 sectors: 1. Ukrainian, 2. Polish, 3. Slovak, 4. Hungarian, 5 Romanian, 6. Polarisation centres, 7. State borders. 8. Administrative limits, 9. Carpathian Euroregion limits).

the interest in trade, economy, culture and administration, sharing Western specific values in compliance with the EU policies related to cross-border matters. The quality and seriousness of the human factor, the maturity and coherence of the achievements are in line with the set objectives. The educational infrastructure follows an optimistic trend, considering the high level of labour force qualification.

THE EUROREGIONS ON THE WESTERN BORDER

In what follows, we will analyse the situation on the western border of Romania, on two distinct lines: the segment of the border between Romania and Hungary, with the Bihor-Hajdú-Bihar Euroregion, therefore consisting of two parties (Romania and Hungary), and the sector of the border between Romania and Serbia, with the Middle Danube-Iron Gates Euroregion, consisting of two parties (Romania and Serbia). As an exception, it will be highlighted the Danube-Criş-Mureş-Tisa Euroregion, a structure consisting of three parties (Romania, Hungary and Serbia)[32]. *Bihor-Hajdú-Bihar* was established in the late 2002, following the simultaneous initiatives of the County Council Bihor

Figure no. 6: the Bihor-Hajdú-Bihar Euroregion[33]

[32] Romanian Academy, Institute of Geography, *op. cit.*, pp. 140-141.

[33] According to Hungary Population Census, apud *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, *loc. cit.*, figure no. 60, p. 152.

and the Local Self-Government of Hajdú-Bihar (Hungary). The practical aspects were set by the *"Concept and Programme of the Romanian-Hungarian Cross-Border Region Development"*[34].

The *Bihor-Hajdú-Bihar* Euroregion is an extremely dynamic and prosperous cross-border structure. The numerous and successful initiatives of the cooperating parties support, through common efforts, the high-level of the border population welfare.

The *Danube-Criş-Mureş-Tisa (DKMT)* was established through the *"Bilateral Cooperation Agreement between Timiş (Romania) and Csongrad (Hungary)"* and the *"Danube-Mureş-Tisa Regional Cooperation Protocol"*, signed in 1997 *(figure no. 7).*

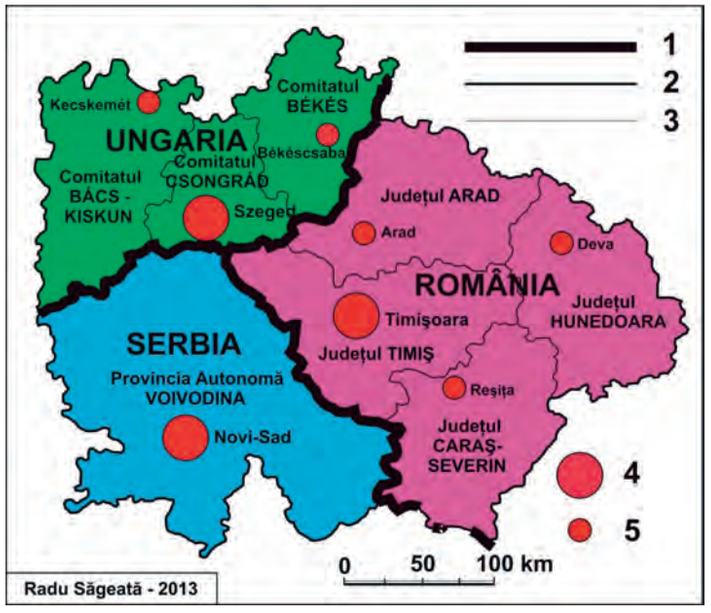

Figure no. 7: the Danube-Criş-Mureş-Tisa Euroregion[35]

The aims are related to the region improved democratisation and the European Union integration acceleration, the social-economic development, the achievement of contacts and special relations in the field of cross-border cooperation. The major objectives are related not only to enhanced mutual relations in the fields of economy,

[34] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 151-155.
[35] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.,* figure no. 70, p. 181.

education and culture, healthcare, science and sports, but also to the collaboration in the field of European integration[36].

The *Middle Danube-Iron Gates* was established on 6 October 2005. In Vidin the constitutive documents were signed, namely the *Association Agreement* and the *Statute of the Middle Danube-Iron Gates Euroregion*. There are involved the Romanian counties Caraş-Severin and Mehedinţi, and the Serbian districts Bor and Branicevski[37] *(Figure no. 8)*.

Figure no. 8: the Middle Danube-Iron Gates Euroregion[38]

Among the efforts of the Euroregion, it is noted the major involvement of the Romanian and Serbian parties in supporting the National Park *"Iron Gates"* (Romania) and, in the mirror, the National Park *"Djerdap"* (Serbia).

The high efficiency of local government policies and the collaboration between authorities, local communities and the business environment

[36] Felicia Dediu, *op. cit.*, p. 212.
[37] Vasile Bogdan, *op. cit.*, pp. 154-157.
[38] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*, *loc. cit.*, figure no. 87, p. 215.

in the spirit of open cooperation, prosperity and progress are illustrative. The developed entrepreneurial spirit, the manifestation of commercial, cultural and administrative exchanges, the operation of successful commercial practices are noted. The awareness of belonging to the levels of civilisation and culture, specific to the West, is certain. Moreover, the accumulated positive experience is used as a bridge to remarkable cross-border results.

The human resource preparation and quality, the mature and responsible approaches are compliant with the tangible set objectives. A feasible and broad education system is developed for the labour force. There are natural and environmental resources that are optimally capitalised on by tourism[39].

THE EUROREGIONS ON THE SOUTHERN BORDER

The system of Euroregions on the southern border comprises the cross-border cooperation structures: the Southern Danube, the Lower Danube, the "Danube 21" Cross-Border Association, the Giurgiu- Ruse, the Danubius and the Danube-Dobrogea.

The system of Euroregions on the southern border comprises the cross-border cooperation structures: *the Southern Danube, the Lower Danube, the "Danube 21" Cross-Border Association, the Giurgiu- Ruse, the Danubius* and *the Danube-Dobrogea*.

The *"Danube 21" Cross-Border Association*[40] was established on 18 January 2002 in Vidin, through the documents signed by the mayors of Calafat, Vidin and Zaječar[41]. The Association is situated at the crossroads of three states (Romania, Bulgaria and Serbia). It has an area of 1,144 km² [42] having localities belonging to three states: *Romania* (the city of Calafat and the communes Desa, Poiana Mare, Ciupercenii Noi and Cetate), *Bulgaria* (the city of Vidin and the communes Macriş, Rujnuti, Lom, Belogradcic, Kula, Novo Selo and Dimovo) and *Serbia* (the city of Zaicear and the communes Kladovo, Sokobania, Bolivat, Bor, Kniajevat and Mandanpec)[43] *(Figure no. 9)*.

It is extremely important the signing, on 1 August 2006, of the *"Agreement between Romania and Bulgaria on the Construction of the Calafat-Vidin Bridge"*, the estimate costs being about 236 million Euros (total costs being 226 million Euros), covered by the European

[39] *Ibidem*, pp. 156-159.
[40] The Association has available all the component and functional particularities that are specific to the Euroregion. The term is in concordance with the smaller area of the presented cross-border structure (A.N.).
[41] Adrian Pop (coord.), *op. cit.*, p. 71.
[42] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 165-169.
[43] Felicia Dediu, *op. cit.*, p. 214.

Union and the European Investment Bank[44]. The 1,971-metre-long bridge was completed on 14 June 2013. The *"Danube 21" Association* is a structure comprising three parties, having an atypical format, the Romanian share being reduced as compared to the Serbian and Bulgarian involvement.

Figure no. 9: the "Danube 21" Cross-Border Association [45]

The *Southern Danube* was established in March 2001, comprising cross-border cooperation structures from Romania (the Local Councils of Alexandria, Turnu Măgurele, Zimnicea and Roşiorii de Vede[46]) and Bulgaria (three urban municipalities: Nikopol, Belene and Veliko-Târnovo[47]).

The Southern Danube was established in March 2001, comprising cross-border cooperation structures from Romania (the Local Councils of Alexandria, Turnu Măgurele, Zimnicea and Roşiorii de Vede) and Bulgaria (three urban municipalities: Nikopol, Belene and Veliko-Târnovo).

The Euroregion activity is less dynamic. The infrastructure development (with the permanent possibility to cross the Danube in the area) could revitalise the economic aspects that are necessary for the highly pauper area.

[44] *Ibidem*, pp. 214- 215.
[45] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*, *loc. cit.*, figure no. 94, p. 237 (1. Romanian sector. 2. Serbian sector. 3. Bulgarian sector. 4. Polarisation centre).
[46] Adrian Pop (coord.), *op. cit.*, p. 71.
[47] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 169-172.

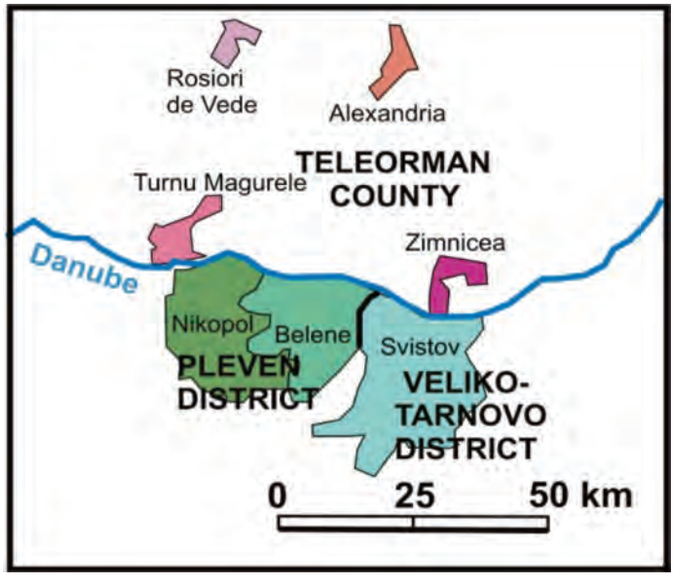

Figure no. 10: the Lower Danube Euroregion[48]

The Danubius was established in 2002 following the joint interests of the County Council Giurgiu (Romania) and the Prefecture in Ruse (Bulgaria). It comprises the Romanian party, with the territory in the Giurgiu County, and the Bulgarian party, with the Ruse province.

The *Giurgiu-Ruse* was established based on the *Establishment Convention*, signed by the mayors of the municipalities of Giurgiu and Ruse on 23 April 2001, in Giurgiu[49].

The Euroregion comprises the City Hall of Giurgiu, the City Hall of Ruse and the Municipal Energy Agency in Ruse (ONG). The Euroregion is situated on the route of strategic trade in former COMECON, Moscow-Kiev-Bucharest, with possible access to Sofia and Burgas, a reason why the Giurgiu-Ruse Bridge was built, between 1952 and 1954.

During the quarterly meetings there are discussed problems related to the environment, healthcare and livestock, requirements or projects being provided rapid solutions in a bilateral format *(Figure no. 11)*. The Euroregion has a small area and reduced possibilities for economic effort and cooperation. However, it maintains the impetus for mutual exchanges and for the effective work of the local administrations in the Danube riverside areas[50].

The *Danubius* was established in 2002 following the joint interests of the County Council Giurgiu (Romania) and the Prefecture in Ruse

[48] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*, *loc. cit.*, figure no. 99, p. 246 (1. Romanian sector. 2. Bulgarian sector. 3. State border).
[49] Ion Talabă, *op. cit.*, p. 195.
[50] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 172-175.

Figure no. 11: the Giurgiu-Ruse Euroregion, administrative structure[51]

(Bulgaria). It comprises the *Romanian party*, with the territory in the Giurgiu County, and the *Bulgarian party*, with the Ruse province[52] *(Figure no. 12).*

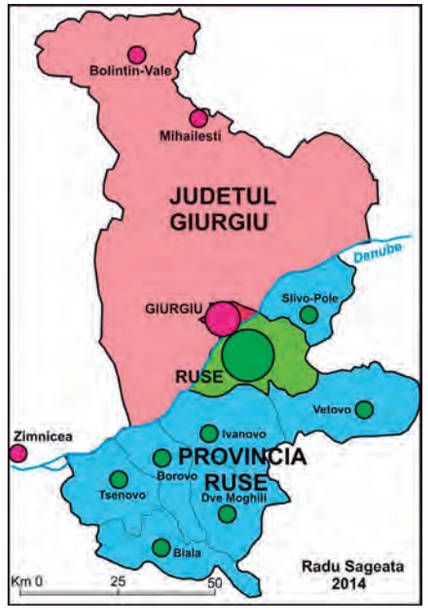

Figure no. 12: the Danubius Euroregion[53]

[51] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.*, figure 102, p. 258.
[52] Ion Talabă, *op. cit.*, p. 196.
[53] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*, *loc. cit.*, figure no. 1072, p. 267.

The *Danubius Euroregion* continues and amplifies the objectives and opportunities previously analysed for the Giurgiu-Ruse Euroregion, but the geographical and economic environment, as well as the demographic structure are extrapolated at the level of the Giurgiu County[54].

The *Danube-Dobrogea* was established in 2002, having territorial structures from Romania (Ialomiţa, Călăraşi and Constanţa counties) and Bulgaria (Silistra and Dobrici provinces – *figure no. 13*).

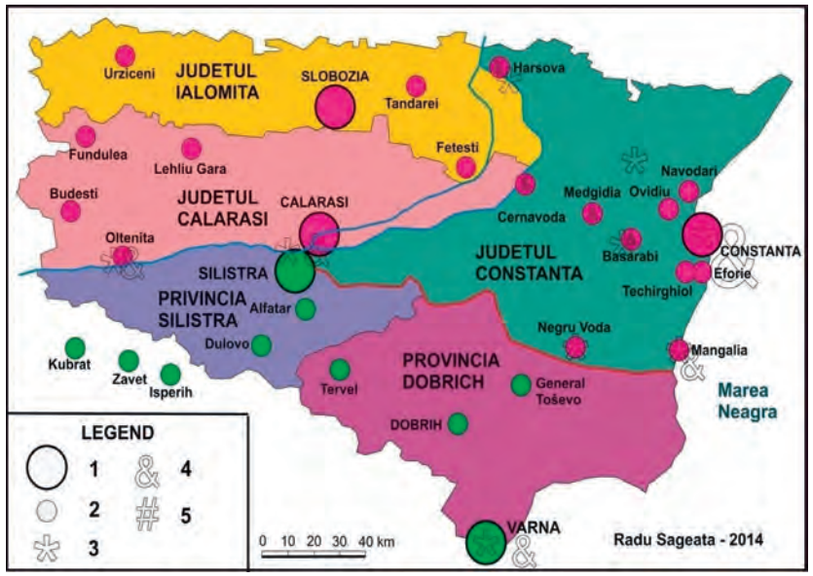

Figure no. 13: the Danube-Dobrogea Euroregion[55]

Within the Euroregions in the south, it is noted the significant involvement of the local communities for cohesion in terms of shaping the space for collaboration, prosperity and progress specific to the Euroregions situated on the southern border of Romania, in compliance with the European Union policies.

The Euroregion is a powerful cross-border structure. The Romanian party comprises Constanţa County, a hub of cross-border polarisation of major regional importance, as a port on the Black Sea. The value of the communications node and of the economic force will increase in the future, in relation to the enlargements of the Rhine-Main-Danube axis, as well as the extension of the hydrocarbon route from the Caspian Sea area.

Within the Euroregions in the south, it is noted the significant involvement of the local communities for cohesion in terms of shaping

[54] Vasile Bogdan, *op. cit.*, pp. 173-175.

[55] According to *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.*, figure no. 118, p. 286. (1. – Regional and local polarisation nuclei. 2. - Ports. 3. - Waterways. 4 – Administrative limits. 5 – State frontiers).

the space for collaboration, prosperity and progress specific to the Euroregions situated on the southern border of Romania, in compliance with the European Union policies.

The entrepreneurial spirit is significant, outlining and manifesting certain forms of commercial, cultural and administrative collaboration, acceptance of EU values and policies in the cross-border field. We note the extension of the positive experience, as an impetus for increased cross-border results.

CONCLUSIONS

The establishment of cross-border structures is a relatively recent reality at the European Union level. The establishment of Euroregions intervenes in areas marked by historical convulsions that have greatly affected the communities located near the borders. Through the mechanisms of cross-border cooperation, the hatred of the past is overcome, being promoted a common construction, as a useful solution, which favors the building of a Europe of peace, detente and progress.

The desired success in the implementation and the future of the Euroregions is dependent on a number of factors, such as the political will of establishing *"bridges"* with former historical enemies, stimulating the entrepreneurial experience and capacity, ensuring multiple support (legislative, political, financial, technological etc.) for the communities involved, supporting the poor areas and accessing European funds, subsidies, donations or tax exemptions, carried out over large periods of time.

For the future, we consider that it is necessary to optimise the European legislative framework, to connect the provisions of the national law to the respective requirements, to direct the planned funds to the areas with poor populations and multiple problems to solve, to establish simplified mechanisms for accessing European funds, to streamline the local decision, to coordinate the practical effort, and to broaden the geopolitical context of affirming cross-border cooperation. Due to the maturity of the long-term effort, the Euroregions can become factors for progress in the future.

From the perspective of national security, the involvement of the Euroregions may have different effects and aspects. Among the positive effects, we can mention the support for increasing the standard

of living, the technological upgrades, the preservation of traditions, the achievement of absolutely necessary critical facilities, the induction of progress and prosperity in less favoured areas. The negative effects refer to the desire to eliminate the borders of the Romanian space, the erasure of national identity, the disappearance of the feeling of belonging to the common past and the elimination of the traditional forms from the cross-border spaces.

BIBLIOGRAPHY:

1. ***, *Law no. 315 on 28 June 2004 (updated) on Regional Development in Romania,* published in the *Official Gazette*, no. 577 on 29 June 2004.
2. ***, *Stadiul actual al reglementărilor naţionale şi comunitare în domeniul cooperării transfrontaliere*, Editura Primus, Oradea.
3. Romanian Academy, Institute of Geography, *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării* (coord. Radu Săgeată). *Geographical Study*, Editura Academiei Române, Bucureşti, 2014.
4. Romanian Centre of European Policies, *Contribution to the Partnership for Development between Romania and the Republic of Moldova*, 29 May 2013, Chişinău.
5. European Union, *Practical Guide to Cross-Border Cooperation. Euro Dobrogea*, Constanţa, 2005.
6. Andrei Balînschi, *Problemele şi perspectivele dezvoltării Eurorehiunii "Prutul de Sus" în condiţiile proceselor integrării europene*, in *Euroregiunile. Prezent şi viitor*, Editura Performantica, Iaşi, 2005.
7. Vasile Bogdan, *Euroregiuni de cooperare transfrontalieră ale României,* Editura CTEA, Bucureşti, 2019.
8. Vasile Bogdan, Emanuel-Ştefan Marinescu, *Cooperarea transfrontalieră şi studii de arie. Curs*, Editura CTEA, Bucureşti, 2019.
9. Tiberiu Brăilean, *Dezvoltare regională şi cooperare transfrontalieră*, Editura Junimea, Iaşi, 2007.
10. Felicia Dediu, *Participarea României la realizarea unor iniţiative în domeniul cooperării tranfrontaliere regionale,* in *"Carol I"* NDU Bulletin, no. 4/2007.
11. Cristina Dogot, *Romanian Local Administrations and Their Activities in the Carpathian Euroregion,* in *Cross- Border Cooperation. Models of Good Practice in the Carpathian Region* (Adrian-Claudiu Popoviciu, editor), Editura CH Beck, Oradea, 2014.
12. Adrian Pop (coord.), Dan Manoleli, *Spre o strategie europeană în bazinul Mării Negre. Cooperarea teritorială,* Institutul European din România, Bucureşti, 2008.

13. Cosmin Sabău, *Efectele benefice ale cooperării transfrontaliere în euroregiuni: Euroregiunea Bihor-Hajdú-Bihar*, Editura Mirton, Timişoara, 2012.
14. Ion Talabă, *România şi tematica euroregiunilor*, in *Euroregiunile. Prezent şi viitor*, *loc. cit.*
15. http://www.interreg-danube.eu/
16. http://www.danube-region.eu/.

ROMANIAN MILITARY THINKING

ROMANIAN MILITARY THINKING

THE NEED FOR PREPARING THE CITY FOR THE CONDUCT OF MILITARY OPERATIONS

Lecturer Sorina-Georgiana RUSU, PhD
University of Architecture "Ion Mincu", Bucharest

Urbanisation has a direct influence on the security and defence field. Military operations tend to take place, with increasing frequency, in the complex environment of contemporary cities. In order to fight in this environment, it is necessary, first of all, to understand the similarities and differences between cities. Each city requires a unique approach, starting from the strategic level of planning, to the tactical level. At the same time, the cooperation of civil and military planners is needed in order to create a common legal framework for the design and defence of cities.

Keywords: urbanisation, civil-military planning, smart city, offensive city, military operations in urban areas.

INTRODUCTION

The way cities develop and expand has an overwhelming importance on the future of human existence. Cities are in a process of continuous transformation, which entails preserving some elements while renouncing others, in order to develop and modernise. There is an extraordinary diversity of urban landscapes today and this makes the preparation of military operations in this environment difficult and extremely challenging.

The increasing connection of cities leads to their increased complexity, interdependencies and vulnerabilities. Finding specific solutions in response to any possible conflict situation is an inappropriate approach. The approach that is required, in the context of the third millennium, is that of prevention, of thinking of urban planning in correlation with military planning.

The diversification of the enemy's typology, in the context of escalating conflicts generated by terrorist actions, also brings to mind the idea of globalising communications, which implies the free flow of information. Although it seems to be a virtue of the modern world, which belongs to the high degree of civilisation, this explosion of information flow is one of the vulnerabilities of post-modernity. Thus, the friend-foe dichotomy, specific to the classical war, should be replaced with the idea of permanent protection of the population, by eliminating the front-line concept, which, as it is known, separates the two conflicting categories: attackers and attacked[1].

Some of the questions that the pre-conflict analysis has to consider are related to the city's planning for a balanced and safe development of the methods to evacuate the city in case of imminent danger and to defend the city, considering how it could be attacked and reconstructed post-conflict, the sites to protect inside the city, the vital internal and external flows of the city.

The diversification of the enemy's typology, in the context of escalating conflicts generated by terrorist actions, also brings to mind the idea of globalising communications, which implies the free flow of information. Although it seems to be a virtue of the modern world, which belongs to the high degree of civilisation, this explosion of information flow is one of the vulnerabilities of post-modernity.

[1] Sorina-Georgiana Rusu, *Planificarea și proiectarea obiectivelor destinate apărării în orașul inteligent*, Editura Paralela 45, Pitești, 2018, p. 109.

URBANISATION AND SECURITY

Worldwide, a historic transition is underway. More than half of the world's population currently live in cities, and the rate of migration is accelerated. By 2030, cities will represent 60% of the world's population and produce 70% of the world GDP[2]. Every day, about 180,000 people around the globe migrate to cities[3]. The urbanisation at such an accelerated rate, especially in developing countries, has an effect on the way cities are configured as well as on their defence.

More than half of the world's population currently live in cities, and the rate of migration is accelerated. By 2030, cities will represent 60% of the world's population and produce 70% of the world GDP. Every day, about 180,000 people around the globe migrate to cities. The urbanisation at such an accelerated rate, especially in developing countries, has an effect on the way cities are configured as well as on their defence.

Cities have distinct, unique, individual similarities and characteristics that require a personalised defence approach. The similarities are given by the elements of urban life and those of urban framework. All the activities located in cities make the urban life (activities, behaviours), while the spaces related to the localisation make the urban framework (spatial configuration, urban culture, urban policy)[4]. The urban life and the urban framework are interdependent, the first element being the engine of transformation, which can take both the form of involution and the form of evolution at the city level.

As Le Corbusier points out, in 1980, "*The great city commands everything, peace, war, work*"[5]. Today we are talking about the existence of urban settlements such as the metropolis[6] or the megalopolis[7], particularly complex environments, in which a new approach to urban planning, related to ensuring the security of the inhabitants, is needed.

[2] United Nations, *World Urbanization Prospects*, 2011, Department of Economic and Social Affairs, New York, http://esa.un.org/unup/pdf/WUP2011_Highlights.pdf, retrieved on 23.03.2020.

[3] United States Agency for International Development, USAID Policy, October 2013, *Sustainable Service Delivery in an Increasingly Urbanized World*, p. 3, https://www.usaid.gov/sites/default/files/documents/1870/USAIDSustainableUrbanServicesPolicy.pdf, retrieved on 20.03.2020.

[4] Alexandru M. Sandu, *Teoria sistemelor urbane – part I,* University Course, Editura Institutul de Arhitectură *"Ion Mincu"*, București, 1975.

[5] Le Corbusier, *Urbanisme,* Flammarion, Paris, 1980, p.78.

[6] The major metropolises are defined by equipment and by areas of influence, the latter defining a threshold of profitability required for high-level equipment (transport infrastructure, reception capacities, political, economic and cultural decision-making institutions, services for large international companies). There are more relationships between international metropolises than between a capital and the cities in its metropolitan area. The size of the metropolitan areas leads to the exacerbation of urban problems (segregation, unemployment, insecurity, land pressure and real estate speculation, degradation of environmental quality), in Jacques Bonnet, *Marile Metropole Mondiale,* Institutul European, Iași, 2000.

[7] *Giant urban ensemble, the result of multiple and complex conurbations taking the form of a continuous city, which was formed when the rural intersections between metropolitan areas were swallowed by urban growth*, in Cătălin Zamfir, Lazăr Vlăsceanu (eds.), *Dicționar de sociologie*, Editura Babel, 1993.

"Overwhelmed by disparities, affected by the multiple major ecological disasters, to which is added the diversification of the range of conflicts that appear either because of the social inequities that favour criminality or because of the escalation of armed conflicts of terrorist type, the contemporary cities must build a defence component. Increasing ethnic, cultural, religious, commercial, economic diversity in general has become a space for conflict generation, especially in areas where managing the situation at the level of governance has not proven the diplomacy needed in such a context. Unfortunately, violence defines some urban communities, and the state of insecurity is the major threat to the peaceful citizen" [8].

In recent years, within the US military, there has been increased focus on settlements of tens of millions of inhabitants. In 2014, the US Armed Forces conducted a research project[9] on the big cities, which essentially concluded that the armed forces are *"poorly prepared"* to conduct any mission and to function in such a complex environment.

ARMED CONFRONTATION IN CONTEMPORARY CITIES

The contemporary city is dependent on the technical infrastructure necessary to support modern urban life, this element also making it vulnerable to attackers. The increasing urban density, together with the anonymity that the big cities provide, makes it difficult to manage these environments, in general, and from the perspective of defence, in particular. Major problems arise both in terms of costs and the complication of the general situation of the classification of urban settlements, in relation to the concept of smart city[10].

The contemporary city is dependent on the technical infrastructure necessary to support modern urban life, this element also making it vulnerable to attackers. The increasing urban density, together with the anonymity that the big cities provide, makes it difficult to manage these environments, in general, and from the perspective of defence, in particular.

The number of terrorist attacks was relatively low in 2012, with 6,771 attacks globally. In just two years, in 2014, the number of terrorist attacks doubled, reaching to 13,463. Most acts of terrorism were located in countries in the Middle East, such as Iraq, and Southeast Asia (Pakistan), where there were 2,965 attacks and 734 attacks respectively. Continuing the analysis of the situation for the following years, the Action on Armed Violence concludes that, during the period

[8] Sorina Georgiana Rusu, *Planificarea și proiectarea obiectivelor destinate apărării în orașul inteligent*, *op. cit.*, p. 58.

[9] See https://api.army.mil/e2/c/downloads/351235.pdf, retrieved on 10.02.2020.

[10] Smart means intelligent. The word is also an acronym, which concentrates the concepts of Specificity, Measurability, Adjustability, Feasibility and Time. These concepts are, at the same time, reference elements on which the city of the future is built – smart city.

January-November 2016, 236 kamikazes acted by detonating explosive charges and causing the death of 11,621 civilians, increasing the percentage of suicide attacks by 19% and the number of victims by 78%[11]. The psychological impact of such attacks on the population is at emotional level, also because of the effect of mental contagion and suggestibility that propagate extremely quickly through online media.

The dynamics of economic powers continuously create disparities and make certain areas vulnerable[12]. That is why it is necessary to propose intelligent solutions to protect the population and resources, by paying special attention to investment in security and defence. Therefore, this is a fundamental argument for the concept of urbanisation of war and for the need to create specialised management structures that ensure the smart planning of cities, having the effect of defending the population, as well as material and spiritual values.

The dynamics of economic powers continuously create disparities and make certain areas vulnerable. That is why it is necessary to propose intelligent solutions to protect the population and resources, by paying special attention to investment in security and defence.

The new military urbanism[13] requires a way of thinking that involves the concern for how to organise and prepare cities for military operations inside them. It is a complex and multidimensional process, although its components are as old as the war itself.

SMART URBAN DEVELOPMENT FOR SAFER CITIES

In order to make cities safer for their inhabitants, it is necessary to inform, educate and train the population to understand the new security challenges and to understand the risk in the context of living in the urban environment.

Given the rise of smart cities, the space saving needed in the localities, the fact that the appearance of the building is no longer mandatory in relation to the functions it can perform and considering the possibility of using the buildings for multiple purposes (multifunctionality/functional reconversion), we consider that modern,

[11] See https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/, retrieved on 03.02.2020.

[12] China's economic growth is expected to slow by up to 4.5% in the first quarter of 2020 – the slowest pace since the financial crisis, because of the new coronavirus in Wuhan, COVID-19 and the epidemic spreading throughout the world. See https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel/, retrieved on 20.02.2020

[13] Fundamental to the new military urbanism is the paradigmatic change that makes the public and private spaces of the cities, as well as their infrastructure – together with the civilian population – a source of targets and threats. See Stephen Graham, *Cities under Siege*, *the New Military Urbanism*, Verso Books, London and New York, 2012.

flexible, and adaptable to the defence requirements cities are necessary, at the same time able to satisfy both the needs of the armed forces in a cost-effective way and the daily comfort of the inhabitants in peacetime. It is important for the inhabitants of the urban settlements to feel the effect of the protection that the secure urban space can offer. In this postmodern context, we consider that the city needs to build and strengthen the intelligence dimension, with the role of intimidating the enemy actions, sliding towards the transition from the concept of defensive city to that of offensive smart city.

Moreover, the new standards for green and smart buildings[14] assist in the construction of buildings in accordance with the principles of sustainable development. Without having the claim of completeness, we consider that at the urban level, besides the specific defence components, there should be concerns for:

- mitigating cyber risks by smartly designing the city's cyber space;
- construction of flexible buildings and infrastructures with a high degree of modularity, allowing, under certain conditions, for multiple use, either for civil or military purposes (by all categories of forces);
- construction of accessible and secure buildings, connected with the defence infrastructure through the application of integrated mobility solutions etc.;
- concealment of military constructions in the urban fabric, with the help of innovative materials, thus reducing the negative psychological impact of their presence on the civilian population[15].

At the level of the elements of urban life it is necessary:

- to analyse the human behaviour in relation to the presence of smart buildings (human logic versus the control system of buildings);
- to replace the friend-foe dichotomy, specific to the classical war, with the idea of permanent protection of the population;

ROMANIAN MILITARY THINKING

Given the rise of smart cities, the space saving needed in the localities, the fact that the appearance of the building is no longer mandatory in relation to the functions it can perform and considering the possibility of using the buildings for multiple purposes, we consider that modern, flexible, and adaptable to the defence requirements cities are necessary, at the same time able to satisfy both the needs of the armed forces in a cost-effective way and the daily comfort of the inhabitants in peacetime. It is important for the inhabitants of the urban settlements to feel the effect of the protection that the secure urban space can offer.

[14] International evaluation systems for green and smart buildings such as BREEAM, LEED, Green Globes, Living Building Challenge etc.

[15] Sorina-Georgiana Rusu, *Cerințe militare și civile în procesul de planificare a obiectivelor destinate apărării în localitățile urbane*, in *Gândirea Militară Românească*, no. 1- 2 (2018), București, 2018, p.77.

- to educate and prepare the population to understand the new security challenges and to act in support of law enforcement, without panicking and destabilising the order of defence actions.

CONCLUSIONS

We believe that the future challenges of urban armed conflicts will focus on a few major elements. They could be: multiplication of mobile threats, process supported by the dissemination of information and the potential access of civilians to different types of databases; emphasis on the phenomenon of population and financial capital migration; possibility of outbreaks of pandemics and the panic that such phenomena create in the collective mind (a recent example is the danger of contamination with Coronavirus); spatial extension of the confrontations in the urban environment, by emphasising the dispersion of the front, in depth and altitude, at the expense of the front of continuous fighting in the urban environment, specific to the classic wars; miniaturisation of weapons, applying nanotechnologies and ensuring the camouflage of newly obtained weapons etc.

The spatial planning of the cities will undergo substantial changes related to the necessity of responding to the challenges that the change of the concept of violence and masked violence implies in an urban environment. The development of dual-use technologies (civil-military) leads to a dangerous simultaneous use of tools and means of combat by civilians and military.

In this context, the spatial planning of the cities will undergo substantial changes related to the necessity of responding to the challenges that the change of the concept of violence and masked violence implies in an urban environment. The development of dual-use technologies (civil-military) leads to a dangerous simultaneous use of tools and means of combat by civilians and military.

In the context of the contemporary world, the ideological, religious beliefs, as well as the level of education and the characteristics of the mass psychology are of great importance in ensuring the defensive capacity of the city. The elements of mass psychology play an essential role, through the invincible power, the mental contagion and the suggestibility that the virtual communities' ability to use the modern means of information are aimed at. Their effective use can be both a threat and an opportunity, at the level of cyber security as well as of the physical environment security[16].

In conclusion, the concern about how to organise and prepare cities for military operations is a need generated by the inevitable, complex and multidimensional process of urbanisation.

[16] Sorina-Georgiana Rusu, *Planificarea și proiectarea obiectivelor destinate apărării în orașul inteligent*, *op. cit*.

BIBLIOGRAPHY:

1. ***, United Nations, *World Urbanization Prospects, 2011*. Department of Economic and Social Affairs, New York.
2. ***, United States Agency for International Development, USAID Policy, *Sustainable Service Delivery in an Increasingly Urbanized World*, October 2013.
3. Jacques Bonnet, *Marile metropole mondiale*, Ed. Institutul European, Iași, 2000.
4. Col. Patrick N. Kaune, civilian research project, *Analysis of US Army Preparation for Megacity Operations*, Institute for National Security and Counterterrorism, US Army War College, Syracuse University, New York, 2016.
5. Stephen Graham*, Cities under Siege, the New Military Urbanism*, London and New York, Verso Books, 2012.
6. Le Corbusier, *Urbanisme*, Flammarion, Paris, 1980.
7. Alexandru M. Sandu, *Teoria sistemelor urbane* – part I, Editura Institutul de Arhitectură *"Ion Mincu"*, București, 1975.
8. Sorina-Georgiana Rusu, *Planificarea și proiectarea obiectivelor destinate apărării în orașul inteligent*, Editura Paralela 45, Pitești, 2018.
9. Sorina-Georgiana Rusu, *Cerințe militare și civile în procesul de planificare a obiectivelor destinate apărării în localitățile urbane*, in *Gândirea Militară Românească,* no. 1- 2 (2018), București, 2018.
10. Cătălin Zamfir, Lazăr Vlăsceanu, *Dicţionar de sociologie*, Editura Babel, București, 1993.

WEBOGRAPHY:

1. http:// esa.un.org/unup/pdf/WUP2011_Highlights.pdf
2. https://www.usaid.gov/sites/default/files/documents/1870/USAIDSustainableUrbanServicesPolicy.pdf3.
3. https://asc.army.mil/web//wp-content/uploads/2015/01/WinComplexWorld-diagram.jpg
4. https://mwi.usma.edu/every-city-different-thats-one-size-fits-approach-urban-operations-wont-work/
5. https://api.army.mil/e2/c/downloads/351235.pdf
6. https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel/
7. https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/
8. https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel/

THE FIXED MARITIME DEFENCE WITHIN THE ROMANIAN SECTOR OF THE BLACK SEA DURING THE INTERWAR PERIOD AND AT THE BEGINNING OF THE SECOND WORLD WAR

Ion RÎȘNOVEANU, PhD
Scientific Researcher 3rd Degree
"King Ferdinand I" National Military Museum

During the interwar period, the political and military decision-making factors in Bucharest made a series of decisions in order to enhance the combative strength of the Romanian Armed Forces, in general, and especially of the War Navy or, since 1931, the Royal Navy.

The economic, political and geostrategic context generated by the end of the Great War and the signing of the peace arrangements within the Paris Conference, which took place between 1919 and 1920, were not meant to ensure Romania with the necessary peace needed for consolidating the National Unitary State.

The revisionist diplomacies of Hungary, Bulgaria and, especially, the Soviet Union led the Romanian political and military decision-makers to adopt a cautious attitude in the relations with neighbouring states that continuously emitted territorial claims over Romania.

Regarding the Romanian maritime coastline defence, although the sums allocated were insufficient, the taken actions temporarily covered the needs of the Maritime Fixed Defence in order to organise a series of coastal batteries which had the role of both protecting the mine fields in front of the Constanța Port and repelling any attempt of enemy troops landing.

Keywords: interwar period, naval doctrine, coastal artillery, Fixed Maritime Defence, Military Navy Command, Royal Navy Command.

INTERNATIONAL CONTEXT

Once the 1918 national unification became a fact, the Kingdom of Romania did not have any more legitimate territorial demands. Given the newly created conditions, in line with the national tradition and in the context of the post-war situation, the concept regarding the dimension of the maritime and river defence of Romania claimed, at least in the beginning, the usage of its armed forces limited to border defence[1].

Given mainly the mentioned context, within the interwar period, Romania had a coherent, yet not extended, naval and coast-line defence policy. Everything was conditioned by the new length of the shoreline, of approximately 250 km, by the direct contact with the open sea or the ocean and by the transport capabilities and long-term battle generating economic power.

Romania was part of the countries lesser preoccupied with the open seas access, having an inferior commercial and military fleet and, implicitly, a smaller degree of tangency to the resources enjoyed by the countries that controlled the world ocean effectively.

The role of artillery in Romanian maritime and river coastline defence and the importance of naval officers' preparation in the field of artillery was a concern of the military analysts even after the end of the Great War.

THE FIRST MEASURES TAKEN BY THE MILITARY NAVY COMMAND TO ORGANISE THE COASTLINE DEFENCE AT THE BEGINNING OF THE INTERWAR PERIOD

The role of artillery in Romanian maritime and river coastline defence and the importance of naval officers' preparation in the field of artillery was a concern of the military analysts even after the end of the Great War. Thus, Captain of the Navy Ioan Bălănescu[2] underlined,

[1] Nicolae Koslinski, Raymond Stănescu, *Marina română în al Doilea Război Mondial,* vol. I., Editura Făt-Frumos, București, 1998, p. 19.

[2] Ministerul de Război (War Ministry), *Anuarul Armatei Române pe anul 1920 (temporary edition)*, SOCEC & Comp., București, 1921, p. 407. Ioan Bălănescu, Captain of the Navy in 1920, was born on 3 July 1878. He graduated the Superior Naval School in 1899, being commissioned as Midshipman on 1 July. Ranks obtained within the service: Sub-Lieutenant (18 May 1906), Lieutenant (10 April 1908), Lieutenant Commander (10 April 1915), Commander (1 September 1917), commissioned as Captain in 1920. Promoted to Vice Admiral, he became Commander of the War Navy between 1934 and 1937.

in an analysis paper on the connections between maritime power and national defence, the importance of defending the coastline by fixed means, mentioning, among others, coastal batteries[3].

Also, Commander Ioan Izbăşescu[4] and Lieutenant Commander Alexandru Gheorghiu[5] drew attention, in 1920, on the role and place of artillery within the Military Navy and on the naval officers' training in this field. The two officers stated that *the artillery has a special importance in the navy and it is necessary for every officer, even if not proficient in artillery, to know how to use this branch of service (…), other than any other speciality, he must pass through an elementary firing directions' course* [6].

The artillery has a special importance in the navy and it is necessary for every officer, even if not proficient in artillery, to know how to use this branch of service, other than any other speciality, he must pass through an elementary firing directions' course

By order of the War Minister No. 15029 from 24 March 1921, the new organisation of the Military Navy comprised, among other structures, the Fixed River Defence and the Fixed Maritime Defence which, next to the Mines Service, torpedoes, wireless stations, as well as the *coastal cannons* or the coastal batteries of the Navy [7].

The Fixed River Defence had also the Armed Barges Group in its composition, which constituted the River Artillery Regiment on 17 November 1920[8].

Within the Fixed River Defence, other than the Armed Barges Group or the floating coastal batteries, as they were sometimes referred to in the period documents, there were also floating batteries for the defence of Galați, Brăila and Sulina Ports. Those subunits had 14 barges in use, each of them armed with a cannon. On 8 barges,

[3] Captain of the Navy Ioan Bălănescu, *Puterea maritimă şi apărarea naţională* , Bucureşti, n/a, p. 18.

[4] Ministerul de Război (War Ministry), *op. cit.*, 1920, p. 407. Commander Ioan Izbășescu was born on 3 March 1881 and graduated the Superior Naval School in 1903, being commissioned as Midshipman on 1 June. Ranks obtained within the service: Sub-Lieutenant (1 June 1906), Lieutenant (1 April 1911), Lieutenant Commander (15 August 1916), Commander (1 September 1917).

[5] *Ibidem*, p. 410. Lieutenant Commander Alexandru Gheorghiu was born on 21 September 1890 and graduated the Naval Academy in Fiume on 6 June 1909 as Midshipman. Ranks obtained within the service: Sub-Lieutenant (3 October 1912), Lieutenant (1 November 1916), Lieutenant Commander (1 September 1916).

[6] Commander I. Izbășescu, Lieutenant Commander Al. A. Gheorghiu, *Dare de seamă asupra stagiului de stat major în escadra franceză în Mediterana occidentală cu concluziuni şi preocupări pentru marina noastră (An Account on the Staff Trial in the French Squadron in the Western Mediterranean with Conclusions and Proposals for our Navy),* Bucureşti. 1940, p. 62.

[7] Arhivele Militare Române (Romanian Military Archives, A.M.R. for short), *Comandamentul Marinei Militare (Military Navy Command)* Collection, folder 388, files 20-21.

[8] *Idem*, folder 290/1920-1921, f. 26.

a 152.4 mm cannon was installed on board, on 4 of them a 120 mm cannon and on 2 barges a 101.6 mm one[9]. Most of those ships were destined for the defence of the Sulina Port.

The floating batteries, as they were sometimes called, had, on 21 December 1920, the following order of battle: 8 barges each with a 152.4 mm cannon on board, four barges with four 120/50 mm cannons and 2 barges with two 101.6 mm cannons each[10]. The *Obukov* 152.4 mm large calibre cannons were captured in 1918 from the Russian fleet dislocated in the Danube Delta area during the Great War together with the barges on board they were placed[11].

The floating batteries, as they were sometimes called, had, on 21 December 1920, the following order of battle: 8 barges each with a 152.4 mm cannon on board, four barges with four 120/50 mm cannons and 2 barges with two 101.6 mm cannons each. The Obukov 152.4 mm large calibre cannons were captured in 1918 from the Russian fleet dislocated in the Danube Delta area during the Great War together with the barges on board they were placed.

Those armed ships were anchored in Galați and Brăila ports, but also in Sulina which, in the interwar period as well as before, represented a strategic point reinforced by Navy artillery and naval units.

For the inland defence of the maritime coastline, limited South in the Balcic area and on the Dniester Firth in the North, the Fixed Maritime Defence was constituted, where the coastal batteries were also found.

EQUIPMENT AND REORGANISATION OF THE FIXED MARITIME DEFENCE DURING THE INTERWAR PERIOD

The Fixed Maritime Defence dedicated sector was situated between the Dniester Firth in the North and the Balcic-Ecrene area in the South with its headquarters in the Constanța garrison. In its new organisation the No. 1 Maritime Sector South which had its area of responsibility the Balcic – Gura Portiţei zone also had in its structure the coastal batteries which began to be deployed on the new line in 1926.

Also, in 1926, the 152.4 mm *Armstrong* cannons belonging to the N.M.S. MĂRĂȘEȘTI and N.M.S. MĂRĂȘTI destroyers were dismounted and sent ashore, to be replaced by more modern ones and placed on the *Tataia* point on the concrete platform and pillboxes built by the Germans during the Great War. In this first shoreline coastal battery four 152.4 mm L/45 *Armstrong* and 76.2 mm L/50 *Armstrong* cannons

[9] *Idem*, folder 308/1916, f.160.

[10] *Ibidem*, f. 160.

[11] Master Sergeant Marin Tănase testimony, serving on this battery from 1926 up until 1946.

were installed in 1926. The 152.4 mm cannons were manned by 8 sailors and the 76.2 mm ones by 6 sailors.

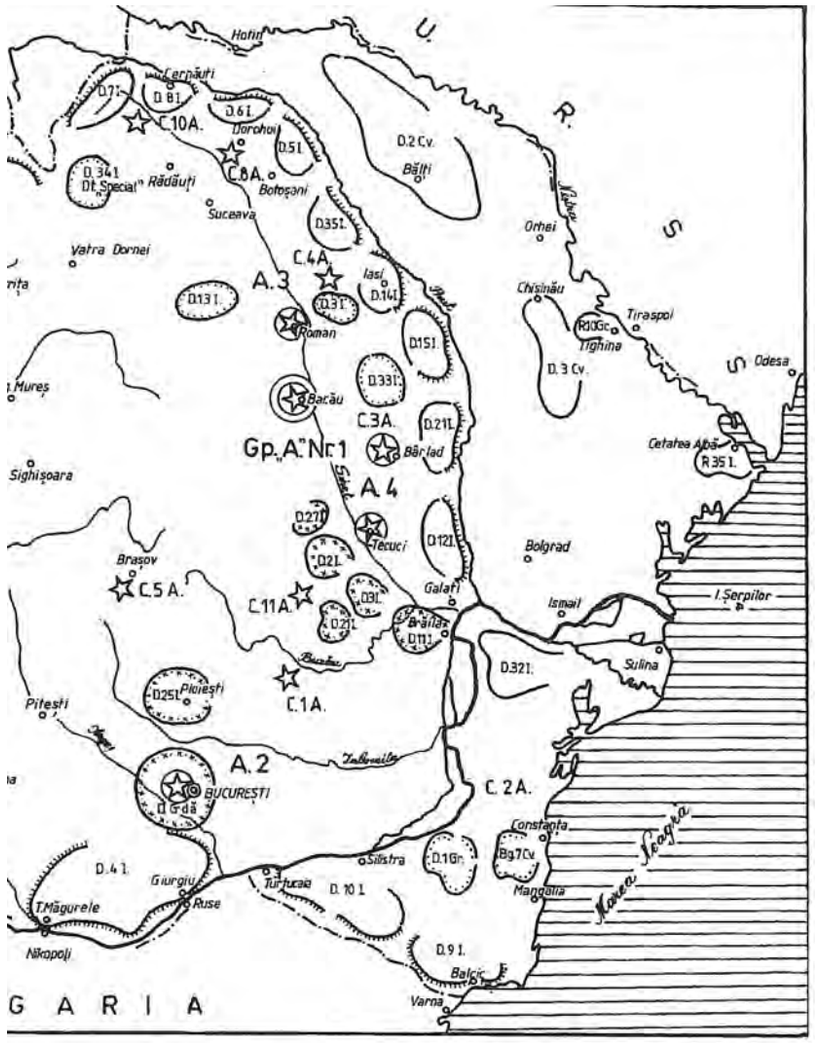

Photo 1: The disposition of the Romanian Armed Forces large units in order to defend Dobruja and the Romanian Black Sea shoreline in the interwar period[12]

[12] A.M.R., *Apărarea Fixă Maritimă/Fixed Maritime Defence* Collection, folder 51/1933-1938, f. 270.

During the same period, along the maritime shoreline, land studies were carried out in order to establish what were the best positions to place the new batteries so that they would assure a good crossfire for the defence of Constanța and the shorelines North and South of the port.

Following the centralised information's study, specialist officers concluded that the best points were Midia, Viile Noi Constanța and Agigea. The land surfaces, where the batteries were going to be deployed, got declared of *public utility* in order to be expropriated[13].

In the *Tataia* Battery, which later became known as *Tudor,* within the armoured pillboxes, the Sea Division's munitions depots were placed. They were supplied by the central depots from Hinog, later moved to Ţăndărei, which, in turn, supplied the entire Navy.

New emplacements and equipment were provided for that battery within the following years. Thus, in 1933 and 1934, the shore was consolidated, where those guns were placed, electric lighting was mounted, telephone lines with the Fixed Maritime Defence Command were established and two anti-aircraft machine gun posts were placed. In 1935, by their own means, a firing and signals dispatch was made active along with bells on each of the four 142.4 mm cannons, thus making it possible for on command firing.

In order to save the 152.4 mm cannon munitions, 37 mm barrels were mounted in the battery, then 6.5 mm weapons for reduced calibre target practice[14].

The first commander of the *Tataia* Battery was Sub-Lieutenant Dumitru Constantinescu, being followed, among others, by Sub-Lieutenant Gheorghe Chiriac, Sub-Lieutenant Ioan Tocineanu, Sub-Lieutenant Haralambie Stănescu, Lieutenant Nicolae Mihalcea, and Lieutenant Marin Tache.

The chief gunner of this battery, from its foundation until 1946, was Sergeant-Major Marin Tănase, who was also the chief of the munitions depot[15].

ROMANIAN MILITARY THINKING

The first commander of the "Tataia" Battery was Sub-Lieutenant Dumitru Constantinescu, being followed, among others, by Sub-Lieutenant Gheorghe Chiriac, Sub-Lieutenant Ioan Tocineanu, Sub-Lieutenant Haralambie Stănescu, Lieutenant Nicolae Mihalcea, and Lieutenant Marin Tache. The chief gunner of this battery, from its foundation until 1946, was Sergeant-Major Marin Tănase, who was also the chief of the munitions depot.

[13] *Ibidem.*
[14] Romanian Navy National Museum's Archives (A.M.N.M.R. for short), *Registrul istoric al Apărării Fixe Maritime/ Fixed Maritime Defence Historical Record.*
[15] *Ibidem.*

Along the seashore, several actions were taken in order to mount other coastal batteries in various points, depending on how the artillery fire crossed in order to have the entire Romanian shoreline in range as well as depending on the defended objectives.

Thus, in 1929, at Capul Midia Point, by Royal Decree, a 76 052 square meters land surface within the Gargalîc (Corbu) rural area, Constanța District, was declared of public utility[16]. Here, the concrete emplacements building for two 152.4 mm *Obukov* batteries began to be built. The four *Obukov* cannons, from the armed barges, stayed stored for many years in the *Tataia* Battery until 1939, when they were mounted in their concrete emplacements.

The battery was organised like a stronghold with ditches and barbed wire around it. It was camouflaged as a small farm with vegetable gardens. For the anti-aircraft defence it had a 20 mm cannon section. Among the *Mircea* Battery commanders, as it became known, we can name Lieutenant Gheorghe Gabroveanu, Lieutenant Anton Petriman, and Lieutenant Marin Trache.

An important moment in the reorganisation of the War Navy was represented by the year 1931. Following the United Kingdom example, by Royal Decree no. 4063 on 15 December 1931, the name War Navy was changed to the Royal Navy and the Military Navy Command was renamed the Royal Navy Command, with command and branch of service inspectorate functions, within the National Defence Ministry.

An important moment in the reorganisation of the War Navy was represented by the year 1931. Following the United Kingdom example, by Royal Decree no. 4063 on 15 December 1931, the name *War Navy* was changed to the *Royal Navy* and the Military Navy Command was renamed the Royal Navy Command, with command and branch of service inspectorate functions, within the National Defence Ministry[17].

Within the forth decade's coastal defence plans, the coastal batteries were involved as well. Thus, a 77 mm battery took part in a training exercise in the Mamaia-Năvodari sector, in September 1932. Its presence was more of a symbolic nature since it had not any munitions, therefore not being able to execute any live fire missions. In the training exercise debriefing, an important conclusion was drawn and that was that small calibre coastal batteries had to be equipped with fast moving means of propulsion in order to become *the mobile element within the firing capability of the coastal defence*[18].

Another coastal battery deployed on the shoreline was the one at Agigea. Work began in 1932 for placing a 120 mm *St. Chamond* battery, but much later, in 1939, three 120 mm *Armstrong* cannons were installed, which were taken from the Cruiser *N.M.S. Elisabeta* and which were also used in the Turtucaia fortifications of 1916. The *Elisabeta* Battery, as it became known, was organised like a stronghold, with ditches, mantles and concrete depots. Among this battery's commanders, best known are Lieutenants Gheorghe Costăchescu and Alexandru Chiriac.

In the 7 September 1932 session, the Royal Navy Committee made an analysis of both the technical situation of the coastal batteries and the necessary number of units to be deployed in the coastal regions. In setting the batteries' needs and placing, the anti-enemy aircraft missions were also taken into account. From the military specialists' studies came out the fact that four 250 mm, four 155 mm, four 120 mm, eight 100 mm and 26 40 mm cannons were needed in the Sulina region. In the Taşaul - Constanța - Tuzla region four 250 mm, eight 155 mm, eight 100 mm as well as 16 40 mm cannons were needed. Also, in the South Tuzla-Ecrene region eight 100 mm and eight 40 mm cannons had to be deployed.

The high cost of the batteries as well as the emplacements works determined the Navy Department within the War Ministry asked for the removal of the 240 mm batteries, which had to be mounted on railway carriages, within the equipment programme. The Royal Navy Committee did not like the requested modifications to be made on the coastal batteries' equipping and organising plan. That is why, in the 27 April 1936 session, the specialists from the Royal Navy Command expressed themselves accordingly, more than that, stating *the wish to have them completed as soon as possible*[19].

[16] A.M.R., *Apărarea Fixă Maritimă/Fixed Maritime Defence* Collection, folder 16, f. 193.
[17] Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Florin Stan, Tanța Mândilă, Andrei Vochițu, Ion Rîșnoveanu, *Istoria Statului Major al Forțelor Navale Române. 1860-2010. Monografie*, Editura Centrului Tehnic Editorial al Armatei, București, 2010, p. 235. See also Captain of the Navy (ret.) (coord.) Anton Bejan, *Dicționar enciclopedic de marină*, Editura Societății Scriitorilor Militari, București, 2006, p. 322.
[18] A.M.R., *Apărarea Fixă Maritimă/Fixed Maritime Defence* Collection, folder 51/1933-1938, ff. 156-157.
[19] *Ibidem*, ff. 156-157.

From a June-October 1932 report on the Fixed Maritime Defence activity, we can learn that, other than the well-placed *Tataia* Battery, all the coastal batteries had *an inefficient deployment on a quantity and quality level in regards to the sensible areas that are to be defended*[20]. Thus, the Midia Battery could not offer full fire coverage to the sector south of Midia Point, which was regarded as the *most sensible point of the coastline*[21].

The committee that analysed the Constanța-Midia strip of shoreline suggested, in a report for the Sea Division, moving the "Tataia" Battery some 500-1000 metres south in order to have better firing coverage of the South Cap Midia sector. The other committee, which analysed the Viile Noi-Mangalia zone, suggested placing the Vii Battery on the high terrace of the Zosima Villa, were, during the 1916-1918 occupation, the Germans had an anti-aircraft battery. It was also proposed that a smaller calibre battery would be placed on a lower position.

Under those circumstances, following minute studies, the Royal Navy Command specialists proposed the battery's relocation by 500-1000 metres to the south, point in which *the 152 mm materiel would fulfil its essential mission*[22].

The *Viile Noi* Battery was not too well placed in the best point for the defence of the Constanța Port either. Its replacement was proposed to be done on the lower terrace of the shoreline from where both better firing and better camouflage were achievable. The movement of the Agigea Battery some 600 metres to the Northeast was also proposed in the document.

Other than the batteries' relocating measures, in the *Committee's Report* it was suggested the reorganisation of the coastal units. They had to be reunited into two groups. One group was supposed to coordinate the batteries north of Constanța, and the other one south of the port, each having its own command structure. At the same time, the report demanded the higher echelons to take definitive actions with regard to the points of deployment for the new coastal batteries and the works themselves.

In the second half of August 1933, two committees conducted new studies on the shoreline for the deployment of coastal batteries. The committee that analysed the Constanța-Midia strip of shoreline suggested, in a report for the Sea Division, moving the *Tataia* Battery some 500-1000 metres south in order to have better firing coverage of the South Cap Midia sector. The other committee, which analysed the Viile Noi-Mangalia zone, suggested placing the *Vii* Battery on the high terrace of the Zosima Villa, were, during the 1916-1918 occupation,

[20] *Ibidem*, folder 33 /1932, f. 101.
[21] *Ibidem*.
[22] *Ibidem*, f. 23.

the Germans had an anti-aircraft battery. It was also proposed that a smaller calibre battery would be placed on a lower position. Studying the Mangalia beaches, the committee postulated that *it would be special for landings* and proposed a special analysis in order to establish the infantry and artillery means needed for the defence of the area[23].

Adding to this, from a report of the Fixed Maritime Command, we can see very clearly that *the tactical possibilities of the Maritime Fixed Defence artillery materiel are very reduced* compared to the length of the strip of shoreline that had to be defended inland.

Out of the 18 cannons assigned to the coastal batteries, only eight were mounted in the field. The other ten were stored in the *Tataia* Battery, their maintenance being very difficult due to lack of funds[24].

Concentrating all the artillery pieces at *Tataia*, whose inventory rose by a few 152 mm cannons delivered in 1933, worried the Fixed Maritime Defence Command, as, in case of an enemy bombardment, they could all have been lost.

Another problem flagged by the Fixed Maritime Defence was that of moving the cannons in bad weather from one position to another as there was not any linking stone road between the Constanța-Mamaia road and the battery[25]. After several requests, 555 tonnes of stone were obtained for the access road building.

The shoreline erosion phenomenon near the *Tataia* point caused justified concern within the Fixed Maritime Defence Command. Taking into account the pieces of information comprised in the presented reports, the Sea Division Commander ordered a land survey. Observing the fact that the danger was real, the battery's relocation was proposed, a request that was approved by the Royal Navy Command.

The shoreline erosion phenomenon near the "Tataia" point caused justified concern within the Fixed Maritime Defence Command. Taking into account the pieces of information comprised in the presented reports, the Sea Division Commander ordered a land survey. Observing the fact that the danger was real, the battery's relocation was proposed, a request that was approved by the Royal Navy Command.

During the interwar period, the *Tataia* Battery had to face other problems too. It needed bonnets for the 75 mm cannons, target mechanisms for the anti-aircraft 76 mm battery as well as munitions for the 77 mm battery.

In regards to training and battle readiness, the *Tataia* Battery results were positively appreciated. For example, on 11 September 1933,

[23] *Ibidem*, f. 23. See also A.M.N.M.R., *Registrul istoric al Apărării Fixe Maritime/ Fixed Maritime Defence Historical Record*, p. 9.
[24] *Ibidem*, f. 35.
[25] *Ibidem*, f. 37.

Vice Admiral Vasile Scodrea, Commander of the Royal Navy, mentioned that the special readiness was *more than satisfying*[26].

Read Admiral Petre Bărbuneanu, the Sea Division's Commander, made the same appreciations, on 16 March 1934. While inspecting the battery, *he was pleased by the obtained results and brought praises*[27], as we can see noted in the *Fixed Maritime Defence Historical Record*[28].

The two commanders' inspections also resulted in carrying out logistical works. Between April and June 1934, the installation of the electrical and telephone network was completed, the cannon sheltering depot was built and the emplacements for the anti-aircraft machine guns were completed on the *Tataia* Battery[29].

Because the necessary munitions for the 152.4 mm cannons could not be provided, during July 1934, 37 mm cannons were fitted and the first day and night target practice-training shots were carried out. On the 3 October 1934 night training shots, Rear Admiral Petre Bărbuneanu was also present. He congratulated the entire battery staff for the manner in which the mission was carried out.

In order to improve the training frame, on 20 October 1934, the Fixed Maritime Defence order of battle was modified. Three training companies were established, one for the 152.4 mm battery, one for the 77 mm section and one for the spotlight section. Attached to the *Tataia* Battery, a telephone, distance and observer training centre was established in order to prepare the necessary personnel for the Royal Navy coastal batteries.

Ensuring the needed munitions allowed for several firing drills to take place in the second half of 1935, with very good results, as well as in earlier years[30]. Along with preparing the gunner and the direct and indirect shots carried out at *Tataia* Battery, by using the firing dispatch and signalling means, the shooting sessions allowed for a constant verification of the respective technique.

A constant concern for the leaders of the Royal Navy up until entering WW2 was to raise the firing capacity of the coastal batteries. On 22 January 1937, the Naval Committee restarted the debate on the possibility of acquiring and installing a 240 mm battery. The offers forwarded by the *Bofors* and *Solothurn* companies were analysed. The matter was analysed in the Navy Committee meeting on 13 October 1937 in which it was stated that the Navy *could not give up the 240 mm battery purchase*[31].

With all the efforts put in, made up by reports sent to the National Defence Ministry, the lack of funds did not permit the purchase and deployment of such a battery. It remained only as something to be desired, the matter being retaken into consideration by the Royal Navy Command on 18 January 1940, when it was decided to place it in the 3rd emergency equipment plan[32].

At the same time, new studies along the shoreline were carried out, having in mind both the cannons positions and the equipment with new batteries. It was believed that, in order to defend the Constanța Port, 7-8 batteries were necessary, out of which four were supposed to be quick firing, two in Constanța and one in Agigea. In the Jibrieni area, five batteries were needed, pointing out that current works mention only one battery[33]. Studies showed that a four-piece battery was needed in Sulina and in Vâlcov, at least a battery with the same capabilities, each needing an anti-aircraft machine gun as well. The study also mentioned that repelling a potential adversary would need *22 artillery pieces, which meant about six batteries of 120-150 mm cannons with a range of 18-20 km.* The document stated that if the fleet had two destroyers with 10 artillery pieces, the number of coastal batteries could be reduced to three[34].

The calculations of the specialist officers from the Royal Navy Command proved that the 22 pieces of artillery equipment plan rose only to 2,361,084,000 lei[35].

Aware of the fact that the budget could not ensure such a sum, the authors of the 1938 study proposed the reinforcement of the coastal battery system by four 150 mm batteries from the Artillery Reserve, six 152 mm cannons from the N.M.S MĂRĂȘTI and N.M.S. MĂRĂȘEȘTI

A constant concern for the leaders of the Royal Navy up until entering WW2 was to raise the firing capacity of the coastal batteries. On 22 January 1937, the Naval Committee restarted the debate on the possibility of acquiring and installing a 240 mm battery. The offers forwarded by the "Bofors" and "Solothurn" companies were analysed. The matter was analysed in the Navy Committee meeting on 13 October 1937 in which it was stated that the Navy could not give up the 240 mm battery purchase.

In order to defend the Constanța Port, 7-8 batteries were necessary, out of which four were supposed to be quick firing, two in Constanța and one in Agigea. In the Jibrieni area, five batteries were needed, pointing out that current works mention only one battery. Studies showed that a four-piece battery was needed in Sulina and in Vâlcov, at least a battery with the same capabilities, each needing an anti-aircraft machine gun as well.

[26] A.M.N.M.R., *loc. cit.*, p. 9.
[27] *Ibidem*, p. 15.
[28] *Ibidem*.
[29] *Ibidem*, p. 19.
[30] *Ibidem*, pp. 29-30.
[31] A.M.R., *Comandamentul Marinei Militare/Military Navy Command* Collection, folder 1221/1940, f. 764.
[32] *Ibidem*, f. 766.
[33] *Idem*, folder 801 /1938, f. 12.
[34] *Ibidem*, f. 12.
[35] *Ibidem*, f. 17.

Destroyers, four cannons from the N.M.S. ELISABETA Cruiser as well as a 75 mm battery[36].

Another commission led by Rear Admiral Izbăşeşcu analysed the defence of the Constanța Port in the field. The idea that the 75 mm *St. Chammond* battery would not be moved to the *Vii* point in the south of the city and that a 47 mm battery, which *would have been placed on the south wall of the oil basin*[37], would take this mission was proposed to the Royal Navy commander.

THE ORGANISATION OF THE COASTAL AREA ARTILLERY OF ROMANIA AT THE END OF THE INTERWAR PERIOD AND THE BEGINNING OF THE SECOND WORLD WAR

The outbreak of the Second World War, on 1 September 1939, with the invasion of Poland by Germany and, especially, Romania's entry into this war on 22 June 1941 against the Soviet Union, imposed on the political and military decision makers from Bucharest the impetuous need to take ample measures to strengthen the capacity to repel a possible enemy landing attempt on the Romanian Black Sea coastline.

The outbreak of the Second World War, on 1 September 1939, with the invasion of Poland by Germany and, especially, Romania's entry into this war on 22 June 1941 against the Soviet Union, imposed on the political and military decision makers from Bucharest the impetuous need to take ample measures to strengthen the capacity to repel a possible enemy landing attempt on the Romanian Black Sea coastline.

A primary measure taken by the Romanian military authorities was linked to the reorganisation of the units that formed the coastal defence. Thus, by the no. 663 Royal Navy Command Order on 12 March 1941, the Coastal Artillery Command was established, a unit whose mission was to organise and lead the Romanian Black Sea coastal defence system.

At the beginning of the 1940s, the Romanian coastal artillery had a morally and physically outdated materiel, which could only partially ensure the protection of the Constanța Port surrounding minefields, let alone repel Soviet naval forces landing in the area.

That is why the German Navy War Mission in Romania, part of the German Military Mission in Bucharest, together with specialist officers from the Romanian Royal Navy Command, conceived a plan to consolidate the Romanian Black Sea coastline defensive system.

To that purpose, the alliance with Germany brought along the deployment of a German coastal battery south of Constanța,

[36] *Ibidem*, f. 22.
[37] *Ibidem*.

in the Lazu village area, called the *Tirpitz* Battery, as well as a mobile railcar mounted battery, known as *Lange Bruno*, in the Mamaia-Sat area.

Thus, in the winter of 1940, six 280 mm SK L/45 cannons were brought to Constanța, sent from the reserves of the *Nassau* class World War One German destroyers.

Three such pieces of artillery entered the *Tirpitz* Battery, deployed in the Lazu area, the remaining three being deployed in the mobile railcar battery north of Constanța[38].

The special deployment works for the battery in the south area of Constanța were completed in the spring of 1941, being also equipped with 88 mm anti-aircraft cannons, 75 mm anti-tank cannons, as well as a motorised unit with the mission of repelling enemy tracked vehicle assaults. Barbed wire fences surrounded the entire base. All was being manned by 600 troops.

The *Lange Bruno* mobile battery, deployed on the railroad north of Constanța, in the Mamaia-Sat area, had the mission of stopping a possible landing on the Mamaia Beach, an easy to assault perimeter due to its large beaches.

Entering active duty in March 1941, the two batteries had the protection of minefield around Constanța Port as a main mission, but also striking the Soviet attacking ships from the distance, ships that might have attacked to produce damage on the city and port or to force a landing.

Each of the six cannons had a weight of 40 t, with a barrel length of 12 m, with a firing speed of three shells per minute. The munition used was in the form of 300 kg heavy 90 cm long shells.

The *Tirpits* Battery went into battle only once, on 26 June 1941, during an attack by a naval formation belonging to the Soviet Black Sea Fleet led by the HARKOV and MOSKVA Command Destroyers[39].

During the action, at 04.22 o'clock, the battery started firing with all three cannons managing, together with the Romanian forces, to repel the Soviet attack.

The special deployment works for the battery in the south area of Constanța were completed in the spring of 1941, being also equipped with 88 mm anti-aircraft cannons, 75 mm anti-tank cannons, as well as a motorised unit with the mission of repelling enemy tracked vehicle assaults. Barbed wire fences surrounded the entire base. All was being manned by 600 troops.

[38] Ioan Damaschin, *Lupta aero-navală de la Constanța din 26 iunie 1941. Cine a scufundat distrugătorul lider MOSKVA?*, Editura Militară, București, 2014, p. 10 and the following.
[39] *Ibidem*, p. 22 and the following. See also Ioan Damaschin, *Război submarin la Marea Neagră*, Editura Militară, București, 2016, p. 21 and the following, and Jürgen Rohwer, *Chronology of the War at Sea. 1939-1945: The Naval History of World War 2*, Naval Institute Press, Annapolis, 2005, p. 83.

CONCLUSIONS

During the interwar period, the Bucharest political and military decision- makers took a series of decisions aimed at strengthening the Romanian Armed Forces combat power, in general, and the War Navy, named the Royal Navy since 1931, especially.

The economic, political and geostrategic context, generated by the end of the Great War and the signing of the Paris Peace Conference arrangements, which took place between 1919 and 1920, was not meant to ensure the necessary peace for Romania to consolidate its National Unified State.

The revisionist diplomacies of Hungary, Bulgaria but, especially, the Soviet Union, made both political and military decision-makers in Romania adopt a careful attitude towards neighbouring states which, continuously, launch territorial claims towards Romania.

The revisionist diplomacies of Hungary, Bulgaria but, especially, the Soviet Union, made both political and military decision-makers in Romania adopt a careful attitude towards neighbouring states which, continuously, launch territorial claims towards Romania.

With regard to the Romanian maritime shoreline defence, all those who held, in the analysed period, the position of commander of the War Navy, the Royal Navy since 1931, were majorly concerned with organising a defensive system in the coastal area meant to discourage a possible armed aggression coming, especially, from the Soviet Union[40].

Although the allocated sums were, on most occasions, insufficient, the taken measures covered, for a while, the needs of the War Navy with regard to preparing some coastal batteries, which had the role of both protecting the minefields in front of Constanța Port and repelling a possible landing of enemy troops.

BIBLIOGRAPHY:

1. ***, Romanian Military Archives, *Comandamentul Marinei Militare* Collection.
2. ***, Romanian Navy National Museum's Archives, *Registrul istoric al Apărării Fixe Maritime*.
3. ***, War Ministry, *Anuarul Armatei Române pe anul 1920 (temporary edition)*, Atelierele Grafice SOCEC&Comp., Societate Anonimă, Bucureşti, 1921.

[40] Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Florin Stan, Tanța Mândilă, Andrei Vochițu, Ion Rîșnoveanu, *op. cit.*, p. 250 and the following. The six admirals who lead the Military Navy, the Royal Navy since 1931, were Vice Admiral Constantin Bălescu (1917-1920), Rear Admiral Constantin Niculescu-Rizea (acting 1920-1921 and full 1921-1925), Vice Admiral Vasile Scodrea (1925-1934), Vice Admiral Ioan Bălănescu (1934-1937), Admiral Petre Bărbuneanu (1937-1940) and Vice Admiral BEng Eugeniu Roșca (1940-1941).

4. Comandor Ioan Bălănescu, *Puterea maritimă şi apărarea naţională,* Bucureşti, f.a.
5. Comandor (r.) Anton Bejan (coord.), *Dicţionar enciclopedic de marină*, Editura Societăţii Scriitorilor Militari, Bucureşti, 2006.
6. Ioan Damaschin, *Lupta aero-navală de la Constanţa din 26 iunie 1941. Cine a scufundat distrugătorul lider MOSKVA?*, Editura Militară, Bucureşti, 2014.
7. Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Florin Stan, Tanţa Mândilă, Andrei Vochiţu, Ion Rîşnoveanu, *Istoria Statului Major al Forţelor Navale Române. 1860-2010. Monografie*, Bucureşti, Editura Centrului Tehnic-Editorial al Armatei, 2010.
8. Căpitan-comandor I. Izbăşescu, locotenent-comandor Al. A. Gheorghiu, *Dare de seamă asupra stagiului de stat major în escadra franceză în Mediterana occidentală cu concluziuni şi preocupări pentru marina noastră,* Bucureşti, 1940.
9. Nicolae Koslinski, Raymond Stănescu, *Marina română în al Doilea Război Mondial,* vol. I., Editura Făt-Frumos, Bucureşti, 1998.
10. Jürgen Rohwer, *Chronology of the War at Sea. 1939-1945: The Naval History of World War 2*, Naval Institute Press, Annapolis, 2005.

NICOLAE ȘTEFĂNESCU – AT THE SERVICE OF THE ROMANIAN STATE AND NATION –

Sorin APARASCHIVEI
"Mihai Viteazul" National Intelligence Agency, Bucharest

Although almost unknown in the historiography of this field, Nicolae Ștefănescu is included in the gallery of famous figures of Romanian espionage and counterespionage. He started his career with the Security Police, where he distinguished himself in identifying and neutralising the Bolshevik espionage organisations. He was head of Foreign Intelligence Service on the USSR within the Directorate of Police and General Security.

His activity being recognised, "as an intelligent and cheerful element", Mihail Moruzov proposed that he should go to the "S" Service of the Romanian Armed Forces, proposition accepted in January 1931, where he would become the head of the Counter-Intelligence Section, as a director. After a few years, he was appointed head of Detectives Corps and director of the Security Police within the General and Police Directorate. His entire activity in the service of the Romanian state and nation is a model of professionalism and commitment.

Keywords: intelligence, Romanian Armed Forces Secret Service, Siguranța Statului (Secret Intelligence Service), Niky Ștefănescu, Detectives Corps.

English version by **Iulia SINGER**.

BIOGRAPHY

Nicolae Ștefănescu or Niky, as he was known among his relatives, was born on 20 September 1896, in Galați. His father was Captain Grigore Ștefănescu, born on 6 June 1871, in Focșani, and his mother, Elisabeta (Eliza), died of tuberculosis when he was five years old, being later raised by his maternal grandmother, Ecaterina Croia. He did not have any siblings, according to archive documents[1]. He graduated from the *"Vasile Alecsandri High School",* in Galați, class of 1916. He claimed, *"but without claiming to be taken serious, that he did a few years of law school".* He had probably studied for a few years, because *"he was able to cope with quite a few problems that required a broader culture"*[2]. He spoke the following languages: French, Russian, Ukrainian, but also some Polish, German, Italian and Serbian.

Photo: Nicolae (Niky) Ștefănescu, in January 1931[3]

In appearance, Niky was of medium height and mobile, *"giving the impression of energy and a pleasant Greek-type physique*", normal size, brown hair, oval face, brown eyes, and as a particular sign he had a scar in the right frontal region. He married Iraida Calimans, in January 1927, a French language teacher at the Girls' Gymnasium in Orhei. His wife's father was an Estonian journalist (former teacher), living in Chișinău.

Obviously, like any great spy biography, Niky Ștefănescu's biography also has some mysteries. Legionary sources claimed that Niky had used false documents in his career, the name of a platoon leader killed

Author's note: the current article is a new research based on primary documentary sources hosted by various archives in our country.

1 Romanian Intelligence Service Archive (ASRI), file no. 20954, vol. 15, pp. 2-4.

2 ASRI, *op. cit.*, *Raport privind pe Niky Ștefănescu*, February 1949, pp. 222-225.

3 *Ibid*.

in the war and that, at his autopsy (November 1940), it was *"established that he was circumcised",* thus facilitating the assumption that he was Jewish, especially since his wife was Jewish (formerly Calimanson)[4].

HIS ACTIVITY WITH THE SECRET INTELLIGENCE SERVICE (1917-1931)

Dumitru C. Dumitru, a childhood friend and former schoolmate of Niky Ștefănescu, confided to a superior from *Siguranța* (the Secret Intelligence Service) that, after primary school, he enrolled in elementary school, but he did not pass the second grade and did not continue[5]. During the World War, Niky joined *Siguranța Statului*, working *"undercover"* at the Shipyard in Galați. In December 1917, however, he *"defected"* and *"joined"* the *Battalion of Romanian Revolutionaries*, under the leadership of famous anarchist Cristian Racovski[6]. Thus, there are striking similarities between Niky Ștefănescu's debut in the *Siguranța* and that of Mihail Moruzov. The latter also *"abandoned"* school in the second grade of high school, due to his infiltration into the youth organisation of the Bulgarian irredentist movement from Dobrogea, becoming, in 1909-1912, a trusted man of the same Cristian Racovski , a position from which he contributed to the discovery of the Russian-Bulgarian espionage activity in Romania.

During the World War, Niky joined Siguranța Statului, working "undercover" at the Shipyard in Galați. In December 1917, however, he "defected" and "joined" the Battalion of Romanian Revolutionaries, under the leadership of famous anarchist Cristian Racovski.

There is probably a kind of truth in all this, because, according to the organisation chart of the Ministry of National Defence, Niky Ștefănescu was hired on 15 April 1918 directly as deputy commissioner of the Tighina Security Brigade of the State Police and General Security Directorate (DPSG), a position that already required some experience and studies. As a police officer, he successively held the following positions: from 1 July 1919, sub-prefect at Cetatea Albă County; of 1 May 1920, deputy special commissioner at the Tighina Security Brigade; of 1 May 1921, deputy special commissioner the Hotin Security Brigade; from May 1922, at Tighina Security Brigade; from March 1923, at Cetatea Albă Security Brigade; from March 1923, at Tighina Security Brigade; from March 1924, at Hotin Security Brigade; from 1 July 1924, he became deputy commissioner first class at the Hotin Security Brigade; of 1 October 1924, at Tighina Security

[4] *Ibid*, pp. 222-225.
[5] *Ibid*, pp. 103-107.
[6] ASRI, file nr. 10988, vol. 1, p. 134.

Brigade; of 1 October 1925, at Iași Security Brigade; of 1 February 1926, at Tighina Security Brigade; from 1 October 1926, special commissioner at the Chișinău Security Inspectorate – as head of the Hotin Security Service; from 1 November 1928, head of the Research Service – Chișinău Security Inspectorate, until 1 January 1931, when he resigned[7].

However, the information missing from the organisation chart was the fact that Niky Ștefănescu was the head of the *Foreign Intelligence Service* of the DPSG on the Soviet space. The appointment in such a position proves that he was a perfect expert in knowing and combating the subversive activity carried out by the Soviet state against Romania. Archive documents reveal that Niky coordinated a strong intelligence and counter-intelligence network across the Nistru River, connecting with the agents through an ingenious system of *"couriers"* covered up as *"smugglers"*. Thus, elements such as Tarak, Vladimir Sabuc or Gr. Ozarciuc are mentioned for using in the assigned missions *"pass permits given by the deputy commissioner Niky Ștefănescu which allowed the freedom of movement in the whole county"*[8]. A report by the DPSG from 12 January 1923 shows that *"several such individuals with a questionable role were discovered and reported to the Cernăuți Security Inspectorate (...), without knowing under what circumstances they passed to the Soviets"*[9].

ROMANIAN MILITARY THINKING

Archive documents reveal that Niky coordinated a strong intelligence and counter-intelligence network across the Nistru River, connecting with the agents through an ingenious system of "couriers" covered up as "smugglers". Thus, elements such as Tarak, Vladimir Sabuc or Gr. Ozarciuc are mentioned for using in the assigned missions "pass permits given by the deputy commissioner Niky Ștefănescu which allowed the freedom of movement in the whole county".

Among the main intelligence elements that made up Niky Ștefănescu's network was Ilie Grigorovici Guțuleac or Huțuleac (called *"Ilinca"*), *"an elite spy"*, as characterised by those who knew him, who also became *"one of Mihail Moruzov's gems"*. Born in 1895, in Polish Galicia (Starojineț County), a Ukrainian, Ilie Guțuleac spoke Russian, German, Polish, Ukrainian and Romanian. A former lieutenant in the Austrian army, he fought in the army of Ukrainian nationalist Simeon Petliura and then in that of Anton Denikin. In April 1920, Guțuleac came to Romania, where he became an agent within the residence of the French Military Intelligence Bureau in Cernăuți, being simultaneously exploited by DPSG and by the Second Romanian Military Bureau. Guțuleac had a *"gang of Ukrainians"* with connections with others in the USSR. Guțuleac's resident from the Camenița-Podolsk point

[7] ASRI, file nr. 20954, vol. 15, The Organisation Chart of the Ministry of National Defence, drawn up in January 1931 by Mihail Moruzov, Head of the *"S" Service*, pp. 226-229 and 245.
[8] ASRI, P Collection, file 10998, vol. 1, p. 137.
[9] *Ibid*, fila 136.

had managed to recruit a GPU (Soviet political police) official. In 1926-1927, Guțuleac appears as *"the head of the Romanian Army Intelligence Centre in Atachi-Soroca",* having the mission to control the activity of the *Soviet intelligence centre* in Iaruga, led by a certain Keppler[10]. One of Guțuleac's tasks, also covered up as a *"smuggler"*, was to set up *"commandos"* whose mission was to attack postmen or bank deposits in order to obtain the money needed to pay our agency and the *"allied"* one across the Dniester[11]. On the other hand, the interest of our special bodies in obtaining Soviet currency is an indicator of the existence of this agency, which had to be paid in local currency so as not to be compromised. At that time, the rubles were difficult to obtain because Romania and the USSR did not have official relations. In fact, Niky and his men were inspired to act in this way by the Soviet regime itself, whose commandos attacked the institutions of the Romanian state and spread terror to the right bank of the Dniester.

By using such tactics and methods, some of Niky Ștefănescu's "smugglers" managed to infiltrate the various organisations of the Soviet state, from where they received instructions and returned to Romania as "Soviet agents". As a result, our special bodies had managed to have some intelligence control over the paramilitary communist cells set up by the Soviet espionage on our national territory.

What is certain is that, by using such tactics and methods, some of Niky Ștefănescu's *"smugglers"* managed to infiltrate the various organisations of the Soviet state, from where they received instructions and returned to Romania as *"Soviet agents"*. As a result, our special bodies had managed to have some intelligence control over the paramilitary communist cells set up by the Soviet espionage on our national territory.

Referring to his activity during this period, Niky Ștefănescu wrote, on 18 July 1924, to his leaders (on the occasion of a promotion): *"In the past, I led an unstable life, which did not lack any dangers (I worked for the Communist Investigation Bureau, both at the Hotin and Tighina Brigades, and at the Chișinău Security Inspectorate), on which occasion I made arrests and investigations throughout Basarabia,* ***operations which did not lack gunfire*** *and from which I believe that the State won (...)"*[12].

Niky Ștefănescu's deeds and bravery in the service of the country are also confirmed by the head of the Hotin Security Brigade, who wanted to highlight the following in his Assessment Paper: *"Old and very good police officer, specialist in investigations. He has led the* ***Foreign Intelligence Service*** *very skilfully; endowed in all his actions*

[10] ASRI, D Collection, file 10988, vol. 1, p. 186.
[11] *Ibid*, file 10988, vol. I, p. 134.
[12] ASRI, file nr. 20954, vol. 18, p. 121.

with much tact and judgment, maintaining a dignified line of conduct both in relations with the staff and with the public outside the service. He is very diligent and punctual at work. Through his enthusiasm for organising the ***Foreign Intelligence Service****, he was able to connect with people from Ukraine who monitored the terrorist gangs in Basarabia, which led to the discovery of the terrorist organisation and the Soviet ammunition depot in Zorojani, Hotin county. For this success, he was proposed for decoration, according to the very verbal order of Minister Tătărescu, by the General Security Inspectorate of Cernăuți. By the same means, the hosts of the terrorist group under the leadership of someone named Puiu were discovered, who, for three years, had been in the GPU service in Cernăuți* [residence, A/N] *and who operated in northern Basarabia, an affair that is currently being investigated by this police officer. Overall qualification grade: very good"*[13].

Suggestive of the dangers to which the Romanian agents were exposed is the *note* by which the command of the I/8 Mountain Troops Battalion asked "*Mr. Niky Ștefănescu whether the Ukrainian agent who gave information about the Zorojani depot is still alive or is one of the two agents killed by Bolsheviks on 3 December 1924"*[14].

TATAR-BUNAR UPRISING: SOVIET ATTACK ON THE ROMANIAN STATE

At the Foreign Intelligence Service, Niky Ștefănescu also had Gheorghe Stârcea, Mihail Cărare, Ion Ajocu and N. Georgescu as team leaders. Together they made an important contribution to counteracting and neutralising the Soviet uprising in Tatar-Bunar (Tătărăști)[15] – the strongest foreign attack on the Romanian state after the war. But they were ready. The information showed that the *Congress of Soviet military agents* took place in Vienna, under the presidency of Egoroff, the commander of Soviet troops on the Southern Front, in this case the commander of the Romanian front, who gave the order to provoke the Bolshevik revolution in Basarabia. And *"if the uprising will engulf the entire Basarabia,* ***irregular troops from the Soviet***

At the Foreign Intelligence Service, Niky Ștefănescu also had Gheorghe Stârcea, Mihail Cărare, Ion Ajocu and N. Georgescu as team leaders. Together they made an important contribution to counteracting and neutraliSing the Soviet uprising in Tatar-Bunar (Tătărăști) – the strongest foreign attack on the Romanian state after the war.

[13] For more details, see Pavel Moraru, *Serviciile secrete și Basarabia, Dicționar 1918-1991*, Editura Militară, București, 2008, p. 291.
[14] ASRI, file nr. 20954, vol. 18, p. 151.
[15] For more details, see Sorin Aparaschivei, *Sistemul național de informații de la Regulamentul Organic și până după Războiul de Reîntregire Națională*, Editura Militară, București, 2018, pp. 411 et seq.

army, concentrated on the Romanian border, will be crossed over the border"[16]. Thus, the Soviet attack on the Romanian state began on 12 September 1924, when the small town of Nicolaevka in Ismail County was attacked by a gang of 25-30 masked individuals, who entered the village and shot the mayor (Jancovski), his wife and two gendarmes (Ion Costin and Gh. Chirvase). The villagers were gathered at the fair (about 1,000 people), where they were read a *manifesto* signed by Terente Colomeez, from the village of Taşlâc, urging them to fight against the Romanian bourgeoisie: *"The bandits were saying that they were not ordinary bandits, but they are part of the Soviet troops that came to fight against the Romanian bourgeoisie".* Then, they attacked the villages Cișmea, Tatar-Bunar (Tătărăști), Vâlcov, Periprava, Nerusai etc.

"The Tatar-Bunar uprising was not the work of the Communist Party of Romania nor a spontaneous pro-Soviet and anti-Romanian manifestation of the local population in Basarabia. It was caused by external circumstances for the following purposes: at the Soviet-Romanian Conference in Vienna, the USSR delegate conditioned the resuming of relations between Romania and the USSR by a plebiscite in Basarabia, adopting a clearly revisionist topic."

Romanian troops intervened and fought fiercely with the bandits, who were very well equipped, being captured thousands of new pistols and rifles of Soviet and German origin, assault cannons, hundreds of grenades, motorboats etc. Hundreds of bandits were arrested and tried. The investigation established that the action was definitely directed against the Romanian state, being organised and financed by the Soviet leadership in Moscow.

Referring to the causes of these events, Niky Ștefănescu considered that: *"The Tatar-Bunar uprising was not the work of the Communist Party of Romania nor a spontaneous pro-Soviet and anti-Romanian manifestation of the local population in Basarabia. It was caused by external circumstances for the following purposes: at the Soviet-Romanian Conference in Vienna, the USSR delegate conditioned the resuming of relations between Romania and the USSR by a plebiscite in Basarabia, adopting a clearly revisionist topic. To the historical-ethnographic arguments of the validity of the Union act, invoked by the Romanian delegate and supported with sympathy by all civilised countries, the USSR opposed a political-social theory, claiming that Basarabia chose a Soviet regime. Since requesting the annexation of Basarabia would have meant cynically distorting the realities, this delegate simply demanded the autonomy of Basarabia. The failure of the Soviet delegates, who, in the absence of arguments, broke off the negotiations, had profound repercussions both on world public opinion and among the Russian*

[16] ASRI, D Collection, file nr. 8348, pp. 7-13.

people. The European states accused the USSR of obstruction and harassment in international relations, and in Russia the tendency to isolate the republic from its neighbours was extremely unfavourably commented. In order to justify the reinstatement of the thesis put forward by the communist delegates, an internationally resounding action was needed to take place in Basarabia. Choosing the region of the subject of this challenge cannot be considered a mere hazard. It was determined precisely by the fact that there was a minority population there, Russians and Bulgarians, who had not begun to be assimilated. ***The organisation of the rebellion was entrusted not to the Basarabian peasants, but to Soviet emissaries who were trained for six months in the leading, leadership and tactics of the civil war*** *[hybrid,* A/N*].* ***The weapons, money and even the literature and stamps of the revolutionary units were made in Russia.*** *The success and even the failure of the Tatar-Bunar rebellion were to confirm the validity of the USSR's point of view at the Vienna Conference.* ***The rebellion failed miserably, highlighting the interference of the Soviet state in organising this revolt*** [emphasis added][17].

The Soviet failure of Tatar-Bunar remains an indicator of the performance of our national intelligence system, which was able to oppose the most dangerous espionage system in the world.

On the other hand, the Soviet failure of Tatar-Bunar remains an indicator of the performance of our national intelligence system, which was able to oppose the most dangerous espionage system in the world.

THE ORGANISATION OF INTELLIGENCE COLLABORATION IN BASARABIA

In Basarabia, Niky Ștefănescu continued to deal with the activity and foreign intelligence collaboration between the DPSG and the Romanian Army bodies, where Mihail Moruzov started his activity as well, being assigned with the organisation of the technical apparatus of the *"S"* Service of the Romanian Armed Forces. Niky Ștefănescu was also responsible for correlating our intelligence bodies with those of the allied residences of the *British Intelligence Service* and the French Bureau II (military intelligence) operating in the Soviet space (tasks were divided, so that there were no overlaps).

[17] ASRI, file nr. 8724, *"Chestiunea Basarabiei, 1930-1939"*, vol. 1, f. 62; Niky Ștefănescu, *cauzele rebeliunii de la Tatar-Bunar*, *raport către Consiliul de Miniștri*, 17 November 1936, document approved by Mihail Moruzov.

By the nature of these duties and tasks, Niky Stefănescu worked more in Chișinău, covered as *"head of the Investigation Service"*, but, according to an internal document of 1 November 1928, he held the position of head of the **Intelligence Office of the General Inspectorate of Basarabia**[18].

Among the landmarks of his activity during this period is the discovery, in March 1928, of the Soviet espionage organisation that had its residence in Nagoreni, Hotin county. The investigation established that the organisation was led by a certain Gh. Draganiuc, who worked according to the directives given by the Soviet *Espionage Office* in Cameniţa-Podolsk (Ukraine), having links with other Soviet espionage centres in Romania, where residents were paid for espionage – all of which were identified and neutralised[19]. Starting from this case, Niky Ștefănescu managed to recruit Vasile Botnariuc (alias Vasile Dogaru), one of the leaders of the Communist Party of Romania. He provided accurate information on the existence, structure, organisation and activity of all communist organisations in northern Basarabia. Dozens of agents of communist paramilitary cells were arrested, some trained in special schools in the USSR, and numerous conspiracy houses, propaganda articles and large quantities of weapons, ammunition and explosives were discovered[20].

Perhaps the most important case investigated by Niky Ștefănescu, as head of the Investigation Service, was that of Commissioner Constantin Tibacu. Niky pointed out that he discovered the case from another lead, a certain Al. Caramanov, a Soviet courier, on which occasion he "discovered the entire espionage organisation under Tibacu's command".

But, perhaps the most important case investigated by Niky Ștefănescu, as head of the *Investigation Service*, was that of Commissioner Constantin Tibacu. Niky pointed out that he discovered the case from another lead, a certain Al. Caramanov, a Soviet courier, on which occasion he *"discovered the entire espionage organisation under Tibacu's command"*[21]. Here, in short, are the facts: Constantin Tibacu was prefect of the Cetatea Albă County (1922) and then head of office at the Chișinău Security Inspectorate[22], therefore a colleague of Niky Ștefănescu. In 1928, on the occasion of the reorganisation of the General State Security, Tibacu's position in Chișinău was eliminated, and he was assigned to a department in Bucharest. But, since his family remained in Chișinău, the new world was not at all familiar to Tibacu. Alone and pressed by financial worries, he tried his best to adapt to the new conditions. The salary was barely enough, around 8-9,000 lei/month, being divided between daily needs, rent and the family left far away. One day in September 1928, Granic (alias name Craiu or Olmozov) appeared in Tibacu's way, a former colleague from the Security in Chișinău, whom he knew had left his job and settled with his family in Berlin. Surprised to see him, Tibacu befriended him. Granic told him that he had left Germany in the meantime and was working in Bucharest, at a large German commercial company, being very well paid. After a few meetings, Tibacu was persuaded to be helped with money by his much better paid friend. He borrowed, with receipts, various sums, which he used to see his family in Chișinău. Then, one day, Granic told Tibacu the truth: *that he was, in fact, a Soviet agent and that he had a mission to recruit him*. Confronted eith Tibacu's refusal, Granic threatened him with the compromising receipts and the fact that he would be killed by the GPU agents accompanying him. Thus, Constantin Tibacu became a Soviet agent. His wife, Reghina, born in Poland, was a very beautiful woman, and the fact that she helped her husband in the activity of betrayal made the investigators believe that she was *"delivered"* to Tibacu by the Soviets, being also sentenced to six months in prison.

ROMANIAN MILITARY THINKING

One day in September 1928, Granic (alias name Craiu or Olmozov) appeared in Tibacu's way, a former colleague from the Security in Chișinău, whom he knew had left his job and settled with his family in Berlin. Surprised to see him, Tibacu befriended him. Granic told him that he had left Germany in the meantime and was working in Bucharest, at a large German commercial company, being very well paid. After a few meetings, Tibacu was persuaded to be helped with money by his much better paid friend.

For testing and initiation, Tibacu went to the Soviet residence in Istanbul, where he met with Visevold Balițki[23], the head of the Ukrainian GPU. Here, in the evening, they spent in luxury hotels, and during the day, Tibacu was trained in the field of encrypting and methods used by the Soviets, and everything went very well, given that Tibacu was already a professional in the field. Balițki told Tibacu that he would have to do everything possible to infiltrate the circle of relatives of Eugen Cristescu, director of State Security. Tibacu's salary was set at 20,000 lei per month, paid in advance, and if he had achievements, he could reach 80,000 lei per month. The money came via Berlin, where, more recently, the headquarters of the Soviet Central, which dealt with Romania, had moved.

The autumn of 1928 and the spring of 1929 were an intense work for Tibacu to thank his new bosses. On the evening of 15 May 1929,

[18] ASRI, file nr. 20954, vol. 4, 1 November 1941, *Moruzov Investigation*, f. 103.
[19] *Ibid,* vol. 18, f. 120.
[20] ASRI, D, file nr. 4702, pp. 100-113.
[21] ASRI, file nr. 6771, *"Soviet Espionage, 1942"*, p. 41.
[22] Almost all newspaper of the time wrote about the *Tibacu-Caramanof Case*, see *"Dimineața"*, 10 May 1930, *"Universul"* or *"Lupta"*.
[23] On 1 August 1931, Balitsky Visevold Apolenovici was promoted among the leadership of GPU Moscow, and his place in the GPU in Ukraine was taken by Stanislav Redens.

Tibacu was partying with his Soviet leaders in Berlin, where he was for a few days for new instructions. One of the Soviets, intoxicated by the drink, confessed to Tibacu that the General Security Inspectorate of Chișinău was infiltrated with the Soviets, that each of the secret reports of the Inspectorate was typed in three copies: one remained at the Inspectorate, the second left for Bucharest, and the third went directly to ... Moscow! Then, surprisingly, Tibacu had the opportunity to meet several of his former colleagues from the Security Inspectorates of Basarabia and Bucovina who now worked for the Soviets.

In Berlin, Tibacu received as new assignments the drawing up of lists with the Romanian personalities from the ministries and the General Security that could have been recruited by the Soviets and well paid. For example, for Eugen Cristescu, in case he could be recruited, the Soviets set a monthly salary of 100,000 lei. In fact, the GPU put agent Kirilov to follow Eugen Cristescu, with the task of recruiting him. When Constantin Tibacu replied to him that the matter was impossible, Kirilov replied to Tibacu that: *"The Soviets have people in Romania to whom he can neither think nor suspect, who will try to recruit Cristescu".*

The Soviets were also interested in Mihail Moruzov and Vintilă Ionescu (the head of counterintelligence in the Security), Tibacu being questioned if he knew them. He answered negatively, although Tibacu, being from Tulcea, knew Mihail Moruzov, with whom he had even been a schoolmate (both had mothers of Bulgarian ethnicity, n.a.). According to Tibacu, the Soviets were worried about the agility of Inspector General Vintilă Ionescu, whom they considered *"the most skilled official of the Romanian Security".*

At the end of 1929, the Soviets ordered Tibacu to steal from the Bucharest Security the file of Constantin Dobrogeanu-Gherea, a former Russian anarchist refugee in Romania, about whom the Soviets learned that he had been denounced to the Security by several Communist Party leaders from Romania (see, above, Vasile Botnariuc, A/N). Those guilty had to be found and lured into the USSR to be punished. As the matter was extremely difficult, the file being stored in Eugen Cristescu's personal filing cabinet, Balițki also arrived in Bucharest. However, the plan could not be implemented and Tibacu missed contacts with his connections in Bucharest. Worried, he went to Chișinău.

At the end of 1929, the Soviets ordered Tibacu to steal from the Bucharest Security the file of Constantin Dobrogeanu-Gherea, a former Russian anarchist refugee in Romania, about whom the Soviets learned that he had been denounced to the Security by several Communist Party leaders from Romania.

On the night of 8 February 1930, after months of investigations and stakeouts, Niky Ștefănescu and security agents from Chișinău knocked on his door to arrest him. Constantin Tibacu was sentenced to 10 years in prison (released in 1938). In the investigation, he tried to minimise his activity, but Niky Ștefănescu and his Service established that he worked under the coordination of important people from Soviet espionage: Leplievscky, from Kharkov, the head of the GPU from all over Ukraine; Vladimir Petrovich Karaolin, Head of Foreign Intelligence (INO) in Kharkov; Vladimir Maximovich Piescariov, head of foreign intelligence in Odessa[24].

However, the investigation into the Tibacu case did not stop here, but shook the entire leadership of the General Security Inspectorate of Basarabia. Mihail Moruzov and the *"S"* Service of the Romanian Armed Forces joined the action, establishing that the main culprit was also Zaharia Husărescu, the head of the Basarabia Security Inspectorate, who was removed from office.

THE CAREER IN THE "S"(ECRET) SERVICE OF THE ROMANIAN ARMED FORCES (1931-1940)

The fact that Niky Ștefănescu was collaborating more and more closely with the Romanian Armed Forces' intelligence bodies, in this case with Mihail Moruzov, was not fully agreed by some Chiefs of the Security. Niky Ștefănescu was accused of all kinds of abuses[25]. In this context, at the end of 1930, Mihail Moruzov made him an offer he could not refuse. Niky Ștefănescu's resignation caused a real shock both in the Security and in the public opinion; even the Russian-language newspaper *"Slova Basarabiei"* headlined*: "Ștefănescu is one of the* ***pillars*** *of Security, he discovered a lot of espionage and communist organisations. He was decorated with a few orders. These days, he was decorated for the second time with the order of the Romanian Crown, and his departure from the Security was something unexpected even for his bosses. Inspector General Maimuca sent a telegram to Bucharest, requesting that Ștefănescu's resignation was not granted"*[26].

On the night of 8 February 1930, after months of investigations and stakeouts, Niky Ștefănescu and security agents from Chișinău knocked on his door to arrest him. Constantin Tibacu was sentenced to 10 years in prison (released in 1938). In the investigation, he tried to minimise his activity, but Niky Ștefănescu and his Service established that he worked under the coordination of important people from Soviet espionage.

[24] ASRI, D Collection, file nr. 7328, *Activitatea SSI român despre activitatea serviciului de informații sovietic în România, Bulgaria, Turcia, Ungaria, Austria (...) anii 1918-1942,* pp. 44-53 et seq.
[25] For more details, see Pavel Moraru, *Serviciile secrete și Basarabia, Dicționar 1918-1991*, *op. cit.*, p. 290.
[26] *Ibid*, p. 293.

So, from 1 January 1931, Niky Ștefănescu moved to the Second Section of the General Staff of the Romanian Armed Forces, where, for some time, Mihail Moruzov organised and led the *"S"* Service – a mixed institution (military and civilian) adapted to the hybrid (political-military) threats proliferated by the Soviet state towards the integrity of the territory and the political regime in Romania.

According to the organisation chart at the Ministry of National Defence (drawn up by Mihail Moruzov), Nicolae Ștefănescu – alias *"I. Popescu"* – was appointed team head at the Secret Service of the General Staff. He filled the following positions: from 1 July 1934, Director Class II (Decision no. 833 S[secret]); from 1 April 1937, Director Class I (Decision No. 355 S) until 5 September 1940, when he was dismissed. Under the *various* heading of the same document it was added: *"N. Ștefănescu was included in the uncovered framework on 22 November 1933, by the Order of the Day no. 141 of the General Staff"*[27].

From 1 January 1931, Niky Ștefănescu moved to the Second Section of the General Staff of the Romanian Armed Forces, where, for some time, Mihail Moruzov organised and led the "S" Service – a mixed institution (military and civilian) adapted to the hybrid (political-military) threats proliferated by the Soviet state towards the integrity of the territory and the political regime in Romania.

At the General Staff of the Romanian Armed Forces, Niky Ștefănescu started his activity at the *Chișinău Intelligence Center ("B")* as an assistant and first collaborator of the head of the centre, Major Constantin A. Râpeanu. The range of action of the *"B"* Centre stretched along the Nistru River, from Atachi-Soroca to Cetatea Albă, with the sole objective of *knowing the political and military situation of the USSR*. Niky worked directly with the heads of agencies in Soroca, Orhei, Lăpușna, Tighina and Akerman (Cetatea Albă). In addition to the informant Vasile Botnariuc mentioned above, he was also helped by Dora Constantinescu, former singer at the operas in Paris and London, who hosted, at the mansion of her estate in Târnava, Soroca county, various people from the fashionable world of the Capital, including Mrs. Seletzki, from the famous Skoda business (in which the Romanian state found out about the double play of the Czechoslovaks in their relationship of *"allies"* with Romania). Niky also continued to work with Ilie Guțuleac, with the Greek Gheorghe Caragunopolus – *"who had bullet marks on his head from a capture he made in Ovidiopol – Ukraine and from which he managed to escape wounded"*[28], with Niculae Cociubei (the Prince) – one of the best spies on the Soviet space, alias

[27] ASRI, P Collection, file 20954, vol. 15, pp. 226-229.
[28] Romania's National Archives/Arhivele Naționale ale României (ANR), Inv. 2349, DGP (General Directorate of the Police), file nr. 58/1920.

"Arghir", part of the Russian aristocracy, gathering information from Russian emigration in Warsaw, Vienna, Hamburg and Berlin.

As entertainment, Niky Ștefănescu also used the world-famous tenor Gogu Ștefănescu as an informant. He performed at *"Radio București"* and frequently toured Italy, France and even Soviet Russia, from where he gathered information for Niky Ștefănescu and Mihail Moruzov. Although, in the documents from the General Staff, they do not appear as having a brother, Niky and Gogu hang around as so at various social events, the great tenor stating to some relatives that he was *"sponsored by his older brother from the Security"*[29].

MAIN COURSES OF ACTION AT THE HEAD OF THE "S" SERVICE OF THE ROMANIAN ARMED FORCES

When Niky Ștefănescu arrived at the *"S"* Service of the Romanian Armed Forces, Section II (Counterintelligence) was headed by a certain *"Vasea Potapov"*, nephew of Mihail Moruzov, about whom the connoisseurs stated that *"he later died in an asylum"*. This was probably the conspiratorial name of Gheorghe Moruzov, a former Security agent and son of the priest Simeon Moruzov, brother of Mihail.

Only in 1932, Niky Ștefănescu was assigned the command of the Counterintelligence Section of the *"S"* Service, especially the counterintelligence side[30]. He was assisted here by Commissioner Gheorghe Comșa, who also joined the armed forces. Within the Service, Niky Ștefănescu was considered the first official after Mihail Moruzov: *"Whenever there was a more difficult mission, which exceeded the counter-intelligence attributions, it was assigned to Niky Ștefănescu. Just as, when it was a more complicated matter, Moruzov, who usually did not consult with anyone, consulted with him"*[31].

In 1932, Niky Ștefănescu was assigned the command of the Counterintelligence Section of the "S" Service, especially the counterintelligence side. He was assisted here by Commissioner Gheorghe Comșa, who also joined the armed forces. Within the Service, Niky Ștefănescu was considered the first official after Mihail Moruzov.

Niky Ștefănescu's priority remained the *"Soviet problem"*. On 20 May 1933, he wrote a report warning that the Soviets were reorganising their espionage apparatus, in which sense they initiated collaborations against Romania with Italian espionage: *"From the information we have, it appears that the Soviets created a Espionage, Propaganda and Agitation Centre in Vienna, whose area of activity includes Romania, Yugoslavia and the Balkan Peninsula. The centre*

[29] ASRI, D Collection, file 10 988, vol. I, p. 134.
[30] ANR, Inv. 2379, file 6/1929, *Statement* – Victor Siminel, p. 7.
[31] ASRI, file nr. 20954, vol. 15, pp. 222-225.

is camouflaged next to the Soviet Embassy in Vienna and has three sections: 1) the Communist Section; the Agitation Section, among the Balkan minorities, including Romania and Yugoslavia; 3) the Espionage Section. The first two sections have special leaders, subordinated to the Soviet representative, the third section was created through the collaboration in terms of espionage of Razvedupr [military espionage, A/N*] with the Italian Espionage Service. To carry out this mission, the section uses as cover by representatives of TASS and IMPRECOR agencies; they are joined by SCHENKER CO. [German]; DERUT [Russian-German company] and RATO [Austro-Russian company], all with headquarters or subsidiaries in Vienna. MOPR [International Red Aid] and the company INTURIST are also helpful"*[32].

As a reaction to the Soviet information hook, Niky Ștefănescu's strategy was to adapt the Romanian counterintelligence to the Soviet espionage in all its dissemination centres.

As a reaction to the Soviet information hook, Niky Ștefănescu's strategy was to adapt the Romanian counterintelligence to the *Soviet espionage in all its dissemination centres, including by penetrating it at his home in the USSR.* For this, the *"S"* Service had to expand its external partnerships for collaboration and exchange of information.

As a result, in June 1933, Niky Ștefănescu met in Belgrade with General Romanovsky and Colonel Durov, former cadres of the Tsarist army (white Russians) who had retreated to Yugoslavia, for the purpose of an anti-Soviet intelligence deal. Niky Ștefănescu reported to Mihail Moruzov the following: *"Gl. Romanovsky, as head of the Russian General Staff, used a number of agents who live today in various European countries. After the coup d'etat of October 1917, he broke off contact with them, but in 1932, together with Durov, he resumed contact with some of them and gathered a series of materials. I think that Romanovsky can be trusted, and Durov, who seems to be an intelligence specialist, is the one who directs the activity of General Romanovsky's intelligence apparatus. Durov is a skilled man, cunning and sensitive to the information given to him. (…) At one point, I asked the two of them to hand me their intelligence apparatus [including in the Soviet space,* A/N*], showing them the immense service they can bring to anti-Soviet ideology.*

(…) I noticed that Romanovsky's intelligence apparatus managed to break into the Soviet Legation [in Vienna, A/N] and that he could get information and photographs about the activity of the Soviets

[32] ASRI, D Collection, file nr. 7181, *Activitatea Kominternului și spionajul sovietic în România și alte țări, 1925-1940*, pp. 148-149.

in Romania. It was agreed that the financing of the Vienna agents should not come under the form of a salary, so as not to turn these people who work only for the sake of the idea into professionals. Durov proposed that the agency's work was directed from Belgrade, but I replied that it could create problems with the Yugoslavs. The solution was reached for Durov to go to Vienna and hand over their agency from the Soviet Legation to our delegate in Vienna, who will have the task of training it on the spot. Romanovsky told me that he also had connections in Prague, but they must be checked, and that he also had connections in the Soviet cities: Kiev, Tiflis, Rostov, Vladicaucaz and Odessa. Romanovsky informed me that he was convinced of the real state of the Romanian-Russian relations and would be willing to start the activity in this direction, provided that complete discretion was ensured, and from the material obtained he would get the part regarding the state of mind in the Red Army and among UTC, and the military materials should return entirely to the Romanians"[33].

From Bulgaria, Niky Ștefănescu established that the main danger for Romania was the Dobrogea Revolutionary Organisation (DRO), of communist orientation, supported and financed clandestinely by both the Bulgarian and the USSR government.

Then, Niky Ștefănescu travelled to Turkey, concluding an anti-Soviet intelligence collaboration agreement here as well. It was agreed that the exchange of information between the *"S"* Service of the Romanian Armed Forces and the General Security in Romania, respectively the Directorate of General Security in Turkey, should take place *"according to the counter-proposals"* of the Turkish party from *"address no. 229 of 20 October 1933",* referring to the *"encryption of telegraphic correspondence"*[34].

From Bulgaria, Niky Ștefănescu established that the main danger for Romania was the Dobrogea Revolutionary Organisation (DRO), of communist orientation, supported and financed clandestinely by both the Bulgarian and the USSR government. The activity of the DRO was coordinated by the Second Section of the General Staff of the Bulgarian Armed Forces, which organized in Silistra a *"center of espionage, propaganda and terror",* placed under the *"orders"* of lawyer Asparuh Aidemirski, President of the DRO, and of Kiril Mauloff, former Bulgarian deputy in the Romanian Parliament, who went to the neighbours in 1928 and was employed by the Bulgarian General Staff. As, in the autumn of 1933, this centre had already started a virulent

[33] *Ibid*, *Report*, 19 June 1933, drawn up by Niky Ștefănescu, Head of *Counterintelligence Section*, pp. 151-153.

[34] ASRI, D Collection, file nr. 9279, vol. 1, p. 158.

action against Romania, the problem was taken over by the *"S"* Service and Mihail Moruzov. It should be noted that, in the matter of DRO, Mihail Moruzov controlled informatively even the wife of the former *"Bulgarian"* senator Hristu Toncof from Bazargic, of Russian origin[35].

THE COOPERATION BETWEEN THE "S" SERVICE AND THE GERMAN ARMED FORCES INTELLIGENCE SERVICE (ABWEHR)

As for Germany, the first collaborations and exchanges of information between the Romanian "S" Service and the German Armed Forces Intelligence Service (Abwehr) took place in the case of Soviet agent Peter Urban. In December 1936, he was found by the "S" Service when he tried to contact officers from the Romanian General Staff and members of the German Legation in Bucharest to offer their services.

As for Germany, the first collaborations and exchanges of information between the Romanian *"S"* Service and the German Armed Forces Intelligence Service *(Abwehr)* took place in the case of Soviet agent Peter Urban. In December 1936, he was found by the *"S"* Service when he tried to contact officers from the Romanian General Staff and members of the German Legation in Bucharest to offer their services. Niky Ștefănescu investigated the case and established that the person was in fact Akoș Domany, a Saxon from Brașov, convicted, two years before, of forgery. While in prison (in Aiud), Domany met Emil Bodnăraș, who came to the USSR in 1934, fraudulently in Romania and who worked intensely in the *Romanian Section* of the Soviet Intelligence Service and in the *Communist International*. Noticing that Akoș Domany was of German origin, Emil Bodnăraș (with a mother of German origin) recruited him and then introduced him to the Soviet Legation through his brother, Emanoil Bodnăraș. The Soviet legation instructed Domany to report to the German Legation in Bucharest and seek to infiltrate the German General Staff, requesting a meeting with important figures on the grounds that he had something pressing to communicate that interested the German General Staff. Von Pochammer, an adviser to the German Legation in Bucharest, fell into the trap of Soviet espionage. He sent Domany to Berlin, informing that he has connections with the Soviet espionage service and that he wished to provide important information to the German General Staff. From Berlin, Domany was sent to Bucharest with a German passport, under the name Urban. Here, he tried to contact the Romanian "S" Service, posing as an envoy of the German General Staff. Through this plan, as Mihail Moruzov later stated, the Soviets wanted to present Urban to the Germans as a Trotskyist (Leon Trotsky was in conflict

[35] ASRI, file nr. 10 998, vol. II, p. 202.

with Stalin, A/N) and thus infiltrate the German General Staff and the Romanian "S" Service, and deliver to them materials *prepared* by Moscow and, at the same time, to gather *"compromising evidence"* regarding the *hidden Romanian-German ties*, and present them to France and Great Britain in order to damage Romania's relations with these states. During the perquisition, an extract from a Soviet plan on the *tactics of the armed insurrection in Romania* (street fight) was found on Urban, a document drafted by Emil Bodnăraș with the help of Soviet agents. It was also established that Emil Bodnăraș made contact, from prison, with Moscow, through the Soviet Legation in Bucharest, which sent him money and instructions through his brother. Emanoil was also the one who brought to the Soviet Legation Emil's reports from prison on the real situation of the Communist Party of Romania following the arrests, as well as other data about the arrested communists and Soviet spies[36].

After completing the investigation in this case, Niky Ștefănescu went to Germany to warn the Abwehr in the matter and, if the Germans were open, to conclude an (anti-Soviet) *intelligence cooperation agreement* between the German service and the *"S"* Service in Romania.

Another circumstance that led to the cementing of our intelligence collaboration with the Germans was the "Dorman case", which took place in the winter of 1936-1937. Dorman (the name was conspiratorial), a former tsarist colonel, pretended to be a "representative" of the Mexican government to make some purchases of old planes from the Romanian state, worth hundreds of millions of lei.

Another circumstance that led to the cementing of our intelligence collaboration with the Germans was the *"Dorman case"*, which took place in the winter of 1936-1937. Dorman (the name was conspiratorial), a former tsarist colonel, pretended to be a *"representative"* of the Mexican government to make some purchases of old planes from the Romanian state, worth hundreds of millions of lei. But the Romanian *"S"* Service discovered that Dorman was, in fact, in the Soviet espionage service, and the purchased planes were taking the road to Spain, where they served to equip the Bolshevik (international) brigades fighting in the *civil war* in this country. The Romanians discovered that Dorman had already made similar acquisitions in Germany, informing the Abwehr in this regard. Niky Ștefănescu left for Berlin, on which occasion he was received by the leadership of the *Gestapo* (the political police of Adolf Hitler's regime)[37].

At the beginning of January 1937, Niky Ștefănescu traveled incognito to Berlin, to set up a meeting with the heads of German espionage.

[36] Information found by the author in a private collection.
[37] ASRI, file nr. 20954, vol. 1-21.

On 21 February 1937, Niky Ștefănescu and his team attended the "Heroes' Day" parade, an event attended by Adolf Hitler himself, accompanied by Marshal August von Mackensen. One of the conclusions reached by the Romanian side was that "the exchange of military intelligence on the USSR, made in the strictest secrecy, was sincere and without reserves, and in the future, the quantity and quality will increase; that the German authorities, in order to have as much information as possible about the USSR, will be willing to make a precise and lasting arrangement".

The following month, a team of the *"S"*(ecret) Service of the Romanian Armed Forces paid a strictly secret visit to the headquarters of the Abwehr, on the *"grounds" of procuring technical equipment necessary for the Service,* but with the real purpose *of establishing contacts of intelligence cooperation on the* (anti-Soviet) *Eastern Front with the German side*. Although he was *"the deputy head of the Secret Service and the head of the Counterintelligence Section",* ie number 2 in the *"S"* Service after Moruzov, this time, Niky Ștefănescu presented himself to the German side as a simple *"public servant, specialist in military matters of the Eastern Front"* , probably under the alias *"I. Popescu"*. In order to confuse the German side, Major Ionescu-Micandru Constantin, accompanied by Capt. BEng Dumitru Son and Capt. BEng Mihai Șerbănescu (the Romanians suspected that the German officers also had conspiratorial names), was introduced as the official head of the Romanian team[38].

Niky Ștefănescu contacted Major von Krienitz, who recommended himself to be the *"assistant"* of Admiral Wilhelm Canaris – the head of the Intelligence Section of the General Staff of the German Armed Forces (Abwehr). The Romanian side also visited the *Gestapo* headquarters, where it was received by Dr Best, who showed his full satisfaction for this beginning of collaboration, especially since Soviet Russia had a common border with Romania, and proposed that BEng Son and BEng Șerbănescu[39] should train in Berlin, at the *Gestapo*, and to use its apparatus. On 21 February 1937, Niky Ștefănescu and his team attended the *"Heroes' Day"* parade, an event attended by Adolf Hitler himself, accompanied by Marshal August von Mackensen. One of the conclusions reached by the Romanian side was that *"the exchange of military intelligence on the USSR, made in the strictest secrecy, was sincere and without reserves, and in the future, the quantity and quality will increase; that the German authorities, in order to have as much information as possible about the USSR, will be willing to make a precise and lasting arrangement"*[40].

[38] ASRI, D, file nr. 3694, pp. 20-32, *Darea de seamă asupra călătoriei la Berlin, 12-24 February 1937*.
[39] On 1 November 1936, BEng Captain Mihai Șerbănescu became deputy of the head of the Technical Service from the *"S"* Service and, together with BENG Captain Son, started to equip the Service with modern technical machines, devices and materials purchased from Germany.
[40] ASRI, D, filenr. 3694, pp. 20-32, *Darea de seamă asupra călătoriei la Berlin, 12-24 februarie 1937*; or ANR, Inv. 2379, file nr. 24/1937, p. 23 et seq.

THE REORGANISATION OF THE COUNTERINTELLIGENCE SECTION

Here are some impressions of Eugen Cristescu regarding the organiser and trainer Niky Ștefănescu: *"Niky Ștefănescu, intelligent and enterprising person, took the Counterintelligence Section out of the routine, completely reorganising it, introduced a series of technical innovations and brought there Scarlat Grigoriu, Ștefan Enescu and Nicolae Stănescu",* future heavy names in Romanian counterintelligence. The *"General Staff also contributes greatly to the reorganisation, both in terms of directives and in terms of investigation plan, and staffing*[41]*. The counterintelligence teams were led directly by Niky Ștefănescu. Those for subversive currents were under the coordination of Gheorghe Comșa; those of stakeout, led by Albu [real name Gheorghe Untăreanu] – Rizescu [Constantin] etc. They consisted of mobile teams, with special organisation, as well as teams for the surveillance and tracking of foreign diplomatic missions. For example, for the surveillance of the diplomatic mission of the USSR, Niky Ștefănescu and Mihail Moruzov formed a special team, consisting of the best elements. At the same time, the teams of the "S" Service infiltrated with special intelligence elements almost our entire diplomatic apparatus from abroad. As a result – Eugen Cristescu underlined -, <The Counterintelligence Section becomes very strong, possessing a numerous staff, thoroughly trained at the Cadres School of the S Service, according to the most modern training methods>"*[42].

"Niky Ștefănescu, intelligent and enterprising person, took the Counterintelligence Section out of the routine, completely reorganising it, introduced a series of technical innovations and brought there Scarlat Grigoriu, Ștefan Enescu and Nicolae Stănescu".

We also add that all this reorganisation was done thoroughly and according to rational, scientific criteria, after consulting a vast documentary material on other intelligence services, especially data on the organisation of the British Intelligence Service, the French II Office and the US FBI, plus data collected on neighbouring intelligence services: Polish, Hungarian, Bulgarian, Serbian and Czechoslovak.

However, this activity met with fierce opposition from the Ministry of Foreign Affairs, especially that of Nicolae Titulescu, who, in 1934-1936, was the dominant factor in our diplomacy and who accused the *"S"* Service of infiltrating the foreign apparatus of the country,

[41] ASRI, file nr. 17474, vol. 1, various statements of Eugen Cristescu, pp. 45-7.
[42] *Ibid*, pp. 7-45.

and that *"diplomatic principles"*[43] are not respected. However, Mihail Moruzov, who did not like the pro-Sovietism shown by Titulescu and did not want any relations with the Soviet regime, channelled almost the entire intelligence and counter-intelligence activity of the "S" Service against the USSR. From the first day after the resumption of diplomatic relations with the Soviets (December 1934), their Legation in Bucharest was subjected to strict surveillance and scrutiny, an action personally led by Niky Ștefănescu[44]. Also, an *"anti-Soviet"* surveillance team, led by Niky Ștefănescu, frequently travelled to the Royal Romanian Legation in Geneva, at the League of Nations headquarters, where Titulescu was active, carrying an *"armored diplomatic bag"* that included a radio station[45].

The Butenko affair: on 6 February 1938, Hrisanfovici Theodor Butenko, the newly appointed Soviet charge d'affaires of the Soviet Legation in Romania, disappeared from his private home. The next day, at 16.00, Vladimir Bodrov, press attaché and representative of "TASS", but also the one who provided counterintelligence surveillance of Soviet personnel, presented himself at the Romanian Ministry of Foreign Affairs to signal the "disappearance" of the diplomat.

Nicolae Titulescu protested against this *"suspicion"* regarding his activity and, seeing that it was not possible to remove the surveillance team, he at least demanded that the team was led by Gheorghe Cristescu, Eugen Cristescu's brother, from Security. Gheorghe Cristescu had been in Paris for several years, sent by Moruzov, to complete his technical specialisation in the *"S"* Service. Titulescu trusted Gheorghe Cristescu, whom he saw as an element formed in the French school, and France, at that time, had developed relations with the Soviets. Through Niky Ștefănescu, Gheorghe Cristescu had succeeded in clandestinely photocopying the Disarmament Protocols for the Geneva Conference, which, at Moruzov's orders, were personally handed over to Nicolae Titulescu, being of great help to the Romanian diplomat in the difficult negotiations in which he participated[46].

BUTENKO AFFAIR

The Butenko affair: on 6 February 1938, Hrisanfovici Theodor Butenko, the newly appointed Soviet charge d'affaires of the Soviet Legation in Romania, disappeared from his private home. The next day, at 16.00, Vladimir Bodrov, press attaché and representative of *"TASS"*, but also the one who provided counterintelligence surveillance of Soviet personnel, presented himself at the Romanian Ministry of Foreign Affairs to signal the *"disappearance"* of the diplomat.

[43] *Ibid*.
[44] *Ibid.*
[45] *Ibid.*
[46] *Ibid.*

In the following days, the Soviet press and the Soviet government attacked virulently from all directions, threatening the Romanian authorities with armed intervention to *"release comrade Butenko"*, characterised as *"a personal friend of Comrade Stalin, kidnapped by the imperialists in Bucharest"*[47].

Then, surprise: on 14 February 1938, the Italian press announced that Butenko was in Rome and that he had left on his own initiative, because he was to be suppressed by a GPU (Soviet political police) agent.

But here are, in short, the facts of this episode: The *"S"* service had certain data that the GPU was going to remove Butenko (through Agent Vasile Thumanov, who arrived from the Soviet Legation in Prague). The Soviet plan provided for an *ultimatum* and possibly an armed intervention for the occupation of Basarabia. Warned by the Romanian side, Butenko *"deserted"* and hid for four days at the home of Mihail Moruzov (17 Sofia Street), where he was questioned by Niky Ștefănescu about Soviet news networks in Romania, agents of influence and so on Also, Th. Butenko left several letters (holographs), in which he expressed the reasons for the gesture. One of them was addressed to King Carol II, a letter from which we read the following passage: *"Sire, leaving the borders of the country, whose destinies are entrusted to Your August hands, I am deeply happy that only on its territory I woke up from the troubled Bolshevik evil dream that had torn my heart for several years.*

(…) In my future career and as a Ukrainian intellectual, wishing happiness for this martyr people, I would be very happy if I could bring the least service to Your Majesty, trusting that between the Bolshevik-free Ukraine and Your Majesty's Kingdom they will be established bonds of close friendship and mutual understanding.

Sire, on 6 February, at 7 o'clock in the evening, I, the head of the Soviet mission in Bucharest, left the building of the USSR Legation forever, to fall at Your Augustus' feet, asking Your Majesty to grant me refuge and bring you my confession, from which it will be seen how I, a 33-year-old Russian citizen, was dragged down the infernal path of Bolshevism, as well as the reasons that determined me to break

[47] ASRI, file nr. 20954, vol. 14, pp. 150 et seq.

free from them. My Person (…)"[48]. Moreover, King Carol II received Th. Butenko in secret.

It is also clear from the documents that Butenko initially demanded the protection of the Octavian Goga government, but Moscow's protest was so vigorous that, in order to ease the situation, our government resigned and it was necessary to negotiate urgently with greater powers, Italy and Germany, to take over Butenko.

On 10 February 1938, at the Jimbolia border crossing, in the table regarding the crossings of people to Yugoslavia, the name *"Niky Ștefănescu, director, Romanian subject"* appears, accompanying a certain *"Mircea Ioan Dobrescu, with passport no. 255014/938, issued by the Ministry of Interior",* none other than... the famous Theodor Butenko, both travellers having as destination Rome!

On 10 February 1938, at the Jimbolia border crossing, in the table regarding the crossings of people to Yugoslavia, the name "Niky Ștefănescu, director, Romanian subject" appears.

But despite the evidence, the Soviets continued to claim that Th. Butenko did not flee, but was abducted and killed, and that the individual in the custody of the Italian authorities was not the real Butenko. Thus, at the request of the Italian authorities, Niky Ștefănescu repeated the visit to Rome to "recognise" Theodor Butenko. In the report to Mihail Moruzov, Niky Ștefănescu describes the brief reunion with Butenko and his surprise to see *"known"* figures.

However, on the occasion of his second trip to Rome, based on the relationships already created, Niky Ștefănescu, on behalf of the *"S"* Service of the Romanian Armed Forces, signed an anti-*Soviet intelligence cooperation agreement* with Italian counterparts. About this mission, Niky reported to Moruzov: *"I went to Rome to check the identity of T. Butenko, on which occasion, on 20 February 1938, I contacted the head of the Intelligence Service of the Italian armed forces, Knight Santo Emanuele, with whom we discussed the need for cooperation in the face of the common danger posed by Moscow's unrest (...). We then set out to take joint action to counter the ongoing Soviet conspiracies and challenges, calling for an exchange of information with Mr Santo Emanuele on the following issues: Soviet political and intelligence activity abroad, directives on strikes and sabotage; Soviet activity and identification of Soviet ties abroad; organisation and deployment of the Red Army (...) ".* On this report, Mihail Moruzov signed and put

[48] *Ibid.*

the following resolution: *"We considered this link necessary, given the needs of the "S" Service for cooperation with common interests"*[49]. The success of the mission in Italy is confirmed in June 1938, when it took place in secret the visit to Romania of the Italian General Valle, the chief of the General Staff of the Italian armed forces, accompanied by Della Porta, the Italian military attaché in Bucharest. On his return, the Italian General sent a congratulatory letter to the General Staff of the Romanian armed Forces for Mr. Nicolae Ștefănescu, for the way in which he took care of the good unfolding of the visit[50].

The success of the mission in Italy is confirmed in June 1938, when it took place in secret the visit to Romania of the Italian General Valle, the chief of the General Staff of the Italian armed forces.

Also during this period, we note that Niky Ștefănescu was sent by Mihail Moruzov to negotiate *intelligence cooperation agreements* with counterparts in Yugoslavia, Greece and Turkey. For example, on 22 June 1938, Niky Ștefănescu received from the Yugoslav state the *"Crown of Yugoslavia"* by Decree of the King of Yugoslavia (communication made to the Romanian side by Yugoslav Lieutenant-Colonel Stropnik – address No. 45889 of 27 January 1939, General Staff, Section II, to the Secret Service)[51].

On 7 February 1940, Niky Ștefănescu was in Yugoslavia again, this time to sign a collaboration and intelligence exchange agreement between the Romanian *"S"* Service and the Yugoslav Security. The intermediary was Ambassador Victor Cădere, who established the necessary contacts with Mr. Vlascalin, *Undersecretary of State in charge of leading the Yugoslav Security*[52].

COMMANDING THE DETECTIVES CORPS AND THEN THE GENERAL SECURITY

The intensification of external risks and threats against Romania determined the state leadership to look for a new formula for streamlining the national intelligence system. Niky Ștefănescu, considered to be a good connoisseur of the realities of State Security, was delegated, in April 1937, to take over the Detective Corps[53] (officially, he was appointed by *ministerial decision* no. 22 267 of August 1938). By law, the Detective Corps had as its attributions the collection

[49] *Ibid*, p. 152.
[50] *Ibid*, p. 232.
[51] *Ibid*, p. 234.
[52] ASRI, file nr. 9060, vol. 2, pp. 5-7; file nr. 20954, vol. 4, regarding the Moruzov investigation, p. 401.
[53] *Ibid*, file nr. 20954, vol. 12, p. 228.

of information by all means: stakeout, informants, telephone and correspondence interceptions etc. from: extremist political parties; national minority organisations, irredentist movements; foreign legations; pursuing espionage suspects; ensuring the security and protection of the royal family and dignitaries[54].

By law, the Detective Corps had as its attributions the collection of information by all means: stakeout, informants, telephone and correspondence interceptions etc. from: extremist political parties; national minority organisations, irredentist movements; foreign legations; pursuing espionage suspects; ensuring the security and protection of the royal family and dignitaries.

From an operational point of view, by appointing Niky Ștefănescu, the Detective Corps (body of the Ministry of Interior) was then subordinated to the *"S"* Service (body of the Ministry of National Defence), meaning that Niky sent daily reports to Moruzov and received major directives from him.

Niky Ștefănescu proved to be an excellent organiser at the Detective Corps as well, especially in the intelligence area. Proof of this are the reports of the time, as follows: *"At Security, Niky Ștefănescu brought a new breath, in large part this being the mentality from the Secret Service, enhanced with his personal contribution. Without going into details, it is enough to say that* ***the most complete internal, political, diplomatic and economic intelligence apparatus, which had been in Romania until then, was the one created at Siguranța by Niky Ștefănescu*** [emphasis added]. *This performance was helped by his professional capacity, which had increased, by the authority of the institution, by the fact that he had a valuable help in the person of Valeriu Ionescu, moved to the Secret Service, as well as by the large funds that had been made available to him"*[55].

Niky Ștefănescu's so-called *"staff"* at the Detective Corps was made up of people brought and trained by him: Paul Abramovici, Tică Gheorghiu, Nicolae Baicu, Petrovici, Borcea, Oproiu, Taflaru, Ghițescu, Wirth, Costel Petrescu, Nae Georgescu, Mănăilă, Curelea etc.[56].

As a result, the successes of the Detective Corps continued: Niky Ștefănescu saved, *"in 10-12 turns",* the life of King Carol II, and according to other versions, even several turns, against the legionnaires' attempts made on the King's life: *"It is not possible to specify in detail where is the merit of Niky Ștefănescu and if the first information regarding the attack, in each of these cases, did not come from Mihail Moruzov himself; but, in any case, the technical instrumentation of the business has always been the merit of Niky Ștefănescu"*[57].

At other times, a *special team* of the Detective Corps *"physically liquidated the conspirators",* which today cannot be overlooked, although the Western services do not lack such examples. Gheorghe Comșa was also part of this *team*, who, although employed in the *"S"* Service, participated in the *"heavy operations of the General Directorate of Police".* The people coordinated by Niky Ștefănescu did not overlook the activity carried out by the National Peasant Party and the Liberal Party, this being sometimes reported at an interval of a few hours away from when something happened inside these historical parties. Apart from this, Niky Ștefănescu's vigilence did not miss *"the activity of Germans, ethnic and passport-bearers, together with that of their organisations, and it was said that perhaps* ***not even in Berlin there was a stricter record of their activity than in the General Directorate of Police*** *[emphasis added]. The economic life also, with all the combinations and underlying things of the different societies, was equally carefully reported, following step by step the infiltration of the German capital, with its political combinations, as well as its rivalry with the western one"*[58].

At the end of June 1940, the Soviet government ordered Romania to abandon Basarabia, threatening with an armed invasion. Hungary and Bulgaria were also threatening Romania. King Carol II asked Germany to guarantee our borders. Our national intelligence system was moving from a state of peace to a state of war, coming under the coordination of the military.

*

But with all this vigilance, some political events could not be prevented, although information did exist. At the end of June 1940, the Soviet government ordered Romania to abandon Basarabia, threatening with an armed invasion. Hungary and Bulgaria were also threatening Romania. King Carol II asked Germany to guarantee our borders. Our national intelligence system was moving from a *state of peace* to a *state of war*, coming under the coordination of the military. As a result, by the Decision of the Minister of Interior no. 46303 of 4 July 1940, Nicolae Ștefănescu, assigned as head of the Detective Corps, was delegated to command the Security Police Directorate of the General Police Directorate[59]. On 13 July of the same year, it

[54] For more details, see Sorin Aparaschivei, *Corpul Detectivilor – Scotland Yard-ul românesc*, available at www.Historia.ro.

[55] ASRI, file nr. 20954, vol. 15, pp. 222-225; Valeriu Ionescu, group head within the "S" Service, then the SSI, had the communists under surveillance, shot himself after 23 August 1944 (A/N).

[56] *Ibid*, file 10998, vol. 1, p. 142.

[57] *Ibid*, file nr. 20954, vol. 15, pp. 222-225.

[58] *Ibid.*

[59] *Ibid*, p. 92.

was issued the decree law no. 49477-S, through which the General Directorate of Police merged with the Gendarmerie Corps and the Capital Police Prefecture into a single body, under the name of the *General Directorate of Police and State Security*. Niky Stefanescu was appointed to lead this institution[60].

But things kept rushing. In the coming months, the *Gestapo* and not *Abwehr* has a say in Romania. The German leadership relied on the *legionary movement*. On 1 September 1940, by Decision no. 61765-S, Niky Ștefănescu was retired from all positions held in the *Siguranță* and returned to his position as head of the *"S"* Service of the Romanian Armed Forces[61].

CONCLUSIONS: THE END AND LEGACY OF NIKY ȘTEFĂNESCU

Niky Ștefănescu was a successful student of Mihail Moruzov, who, to the teachings of his master, added his own police experience and a lively intelligence, with many possibilities to adaptat to different situations.

On 6 September 1940, Mihail Moruzov and Niky Ștefănescu were arrested and imprisoned in Jilava, where, on the night of 26/27 November of that year, were assassinated by legionnaires[62]. Threatened by the legionaries, Iraida Ștefănescu left Bucharest and moved to Basarabia, to Orhei. A note from the Romanian Special Intelligence Service (formerly the *"S"* Service) shows that, during the Soviet occupation of Basarabia, she came under the attention of the Soviet intelligence agencies. After 23 August 1944, Iraida Ștefănescu made several attempts for the Romanian state to grant her a survivor's pension[63].

This is, in short, the biography of Niky Ștefănescu, one of the greatest professionals that Romanian espionage and counterespionage had. Its significance for this field is also revealed by the following archive testimony: *"Niky Ștefănescu was a successful student of Mihail Moruzov, who, to the teachings of his master, added his own police experience and a lively intelligence, with many possibilities to adaptat to different situations.*

He had no political convictions** and, just as he followed the communist movement in Basarabia, so did he pursue the legionaries in Bucharest; **its orientation being only according to the interests

[60] *Ibid*, p. 96.
[61] *Ibid*, p. 99.
[62] ASRI, file nr. 10998, vol. 1, p. 129.
[63] *Ibid*, file nr. 20954, vol. 15, p. 287.

***of the State.** (...) Those who came in contact with him had a lot to gain in the speed of solving the problems and the execution without personal attitudes of the missions received from the established order"*[64].

For his exceptional merits in the service of the Romanian state and nation, Niky Ștefănescu was appreciated at the highest level, being honoured with various decorations, including: *"Bărbăție și Credință Clasa I", "Cavaler al Ordinului Coroana României", "Ofițer al Ordinului Coroana României", "Crucea de Război Franceză"*.

BIBLIOGRAPHY

1. ***, Arhivele Naționale ale României/Romania's National Archives, Inv. 2349, *Direcția Generală a Poliției/Police General Directorate*, files nr.: 58/1920; 6/1929; 24/1937.
2. ***, Arhiva Serviciului Român de Informații/Romanian Intelligence Service Archives, files no.: 3694; 4702; 6771; 7181; 7328; 8348; 8724; 9060; 9279; 10998; 17474; 20954 etc.
3. Pavel Moraru, *Serviciile secrete și Basarabia, Dicționar 1918-1991*, Editura Militară, București, 2008.
4. Sorin Aparaschivei, *Corpul Detectivilor – Scotland Yard-ul românesc*, available at: www.Historia.ro.
5. Sorin Aparaschivei, *Sistemul național de informații de la Regulamentul Organic și până după Războiul de Reîntregire Națională*, Editura Militară, București, 2018.

[64] *Ibid*, pp. 222-225.

THE FRENCH NAVAL MISSION TO ROMANIA – THE EFFORTS MADE FOR SIGNING NAVAL PROCUREMENT CONTRACTS AT THE END OF WORLD WAR I –

Dan-Dragoș SICHIGEA, PhD student

Chief of Mangalia Museum Department, the Romanian National Naval Museum

At the end of World War I, the Romanian Army was experiencing the results of three years of military conflict on its own territory and was also entering into a period of reconstruction. One of its components, the Navy, was also coming to the point of realisation that the new, greater Romania was inevitably going to put more pressure on its Black Sea Division, especially if we take into consideration that the union with Basarabia meant it had to defend a much larger coast. Therefore, the Romanian Naval Inspectorate sought new ways to increase its naval forces, mostly by using the experience of foreign naval officers accredited in Romania. The most active ones were the representatives of the French Naval Mission. They would go on to propose a large array of different ship types for the Romanian Navy.

Keywords: Naval Inspectorate, French Naval Mission to Romania, Military Navy, minesweepers, Royal Navy.

THE BEGGINING OF THE FRENCH MISSION

Starting 1916, France organised a Military Mission to assist its Entente ally, Romania. This would include a naval component, meant to help modernise the small Romanian Navy. A more important fact for France was that it could help guide the Romanians in combat on the Danube against the Central Powers. For this mission, the French sent to Romania three officers: Captain Belloy de Saint-Lienard (who led the mission) and Lieutenants Berg de Breda and Baheze de Lanley[1].

The concrete results of the mission to Romania were quite scarce for the French specialists. Romania's rapid failure to occupy Transylvania led to its catastrophic defeats in 1917 and its exit from the war. This meant that the naval actions on the Danube were quite rare, and successes even rarer.

Romania's strategic position offered interesting posibilities. More so since it had in its possession most of the course of the Danube and the country was very close geographically to Russia.

The French interest for the naval affairs of Eastern Europe and Romania in particular was to return after the country reentered the war in 1918 and captured its lost territories. This was to continue for the next couple of years, during which time Romania was struggling to consolidate its much larger territory. As a possible ally in a naval war in the Black Sea, Romania did not promise much in terms of maritime strength. The Romanian Navy did not have any seaworthy ships to talk about, and despite many plans of expansion, it clearly lacked the funds to support them, at least on the short and even medium term.

Its strategic position, however, was a different story and offered more interesting possibilities. More so since it had in its possession most of the course of the Danube and the country was very close geographically to Russia. These all benefited from special attention from French planners in Eastern Europe. Similar conclusions were reached by the British Navy (The Royal Navy). It was quick to catch up to the French in trying to secure naval influence in the Black Sea area.

Comparatively to the British, the French were already much more invested in this problem and they soon had to allocate more resources

[1] Patrick Boureille, *"Les relations navales franco-roumaines (1919-1928): les illusions perdues"*, in *Revue historique des armees*, 244/2006, p. 2.

to ensure they held a superior position in regards to the influence in the Romanian Navy. The results fell short of their expectations though. By the summer of 1920, Great Britain managed to send its own Naval Mission to Bucharest and it functioned in parallel with the French one, practically making up the disadvantage it had compared to the French. Even more, the British mission was accredited to the War Ministry in Bucharest, which actually was of much higher rank that the French one, which was accredited to the Navy Directorate. We can safely assume that France was losing ground in respect to the British, as far as the Romanian Navy was concerned.

Ever since February 1919, the leadership of the Romanian Navy had asked the French Naval Mission to help it organise a minesweeping service on the coasts of Romania after its calls for help to the other Allied Powers went unanswered. As with those requests, the Romanian Navy just wanted to be handed out some minesweepers, even if temporarily. These would then be operated by Romanian crews to sweep the approaches.

This explains why the French Naval Mission was very busy in trying to find new ways of becoming relevant in the Danube and Black Sea areas. One endeavour would have unforeseen and negative consequences for the French. This was their involvement, which is to say their naval officers, in the different projects of reorganisation of the Romanian Navy. From Captain O'Neill, who replaced Belloy as the chief of the mission at the end of 1919, we can find that the Romanian Naval Inspector, Rear Admiral Constantin Bălescu, did not appreciate the French cooperation and their connections directly with the Romanian Government. He felt that the direct connection between the French and the Government was an intrusion, bypassing him and his staff at the Inspectorate and Directorate level[2].

THE SUBMARIN CHASERS IDEA

A matter that brought some success for the French Naval Mission and also an opportunity to surpass its British rivals was the very difficult task of sweeping the sea mines on the Danube and in the Black Sea. These were left there after the war, and ever since the Central Powers minesweepers retreated, they caused a significant amount of trouble of the shipping in the area. The Romanian Navy was ill equipped to handle this problem, having no real minesweeper for the Danube and its territorial waters in the Black Sea[3].

Ever since February 1919, the leadership of the Romanian Navy had asked the French Naval Mission to help it organise a minesweeping service on the coasts of Romania after its calls for help to the other Allied Powers went unanswered. As with those requests, the Romanian Navy just wanted to be handed out some minesweepers, even if temporarily. These would then be operated by Romanian crews to sweep the approaches. It is clear that the Romanians were eager to exploit the willingness of the French Mission to make up for the ground it had lost and relinquish some ships for that purpose. The Romanian Naval Inspectorate saw some evidence in this regard in the fact that the French kept their ships in the area even during peace times for minesweeping.

The Romanian Navy was eager to create its own sweeping units in the Black Sea, not just to safeguard its navigation routes which were very important for the economic recovery of the country. As Rear Admiral Bălescu pointed out, it was critical to avoid that the Allied Power *"should organise on their own the minesweeping service in our harbors and waters"*[4]. It was a question of national prestige for Romania to avoid relying on foreign ships and this was the reason it tried to get a hold on some vessels and use them with Romanian crews. Romania had goals of becoming a significant power in the Black Sea region and it found it unacceptable to allow foreign powers to sweep its waters: *"this would mean to request and accept a foreign protection in regions that might lead to costly obligations and humiliating servitudes"*[5]. It is quite possible that these remarks also pointed out the resentment that the Naval Inspectorate had towards the foreign naval missions in Romania and their constant involvement in the reorganisation process of the Romanian Navy, an intrusion that caused such problems.

It was a question of national prestige for Romania to avoid relying on foreign ships and this was the reason it tried to get a hold on some vessels and use them with Romanian crews. Romania had goals of becoming a significant power in the Black Sea region and it found it unacceptable to allow foreign powers to sweep its waters

The Navy's plan was to continue the negotiations with the French and create some goodwill by buying some gunboats it had already agreed upon (the *"Chiffone"* type ships). These talks would bear fruit in December 1919, when four of these ships entered Romanian service[6]. The Romanian Navy hoped this goodwill would be used to broker a deal for some minesweepers, lent or given at no cost by the French. If all went as planned, it was thought that the Navy could create three minesweeping divisions[7] as follows:

- the first unit, in the northern, most threatened area, would have been based at Sulina. It would have had two gunboats

[2] *Ibid*, p. 3.

[3] Arhivele Militare Naționale Române/Romanian National Military Archives – AMNR, Military Navy Command Collection, file 270, p. 71.

[4] *Ibid*, f. 69.

[5] *Ibid*, f. 70.

[6] Georgeta Borandă, *"Nave de luptă românești – breviar",* in Ion Ionescu, Georgeta Borandă, Marian Moșneagu, *Noi contribuții la istoria Marinei Militare Române*, Constanța, Editura Muntenia & Leda, 2001, p. 145.

7 AMNR, Military Navy Command Collection, file 270, p. 70.

with sweeping gear, plus six motor boats in the area of Sulina – Akerman;
- the second one, at Constanța, would have had the same number of ships and the same types. Its area of operations was from Constanța to Balcic;
- lastly, the third division, with another two gunboats and six motor boats, was the reserve[8].

One can see that in July 1919, when this plan was created, the Romanian Naval Inspectorate was counting on getting six gunboats. Eventually, however, it could only afford four.

The American Navy wanted a submarine hunter that was cheap and solid, but with a wooden hull. It had to reach speeds of up to 17-18 knots. The planned range was about 1,500 miles and the initial armament consisted of a 76 mm naval gun, a 57 mm one and three machine guns. The lessons learned before that during the war showed that submarine chasers could be limited to actions in coastal water. Instead, they would have to venture in deep waters in pursuit of their targets.

At the same time, the Chief of the French Naval Mission, Captain Belloy de Saint Lienard, was involved in other projects designed to help the Romanian Navy to increase its forces on the seaside. After the Romanians made several inquiries about what ships the French Navy was ready to sell, of course trying to get some good bargains, there were some ideas. The French Mission made some significand efforts in trying to find different solutions for a mutual advantageous solution.

Also in the summer of 1919, taking advantage of the fact that some French submarine chasers (motor boats, to be more precise) were on the Danube on minesweeping missions, the Romanian Naval Inspector, Read Admiral Bălescu was invited to visit one of these ships, *"C 27"*[9].

These ships were actually of American design and build, the project starting back in 1917, when the threat of German submarines was at its peak. The American Navy wanted a submarine hunter that was cheap and solid, but with a wooden hull. It had to reach speeds of up to 17-18 knots. The planned range was about 1,500 miles and the initial armament consisted of a 76 mm naval gun, a 57 mm one and three machine guns. The lessons learned before that during the war showed that submarine chasers could be limited to actions in coastal water. Instead, they would have to venture in deep waters in pursuit of their targets. This led to the idea of slowing the ships down for an increase in machine reliability, the project thus becoming even better[10].

The ships would receive the name of *"S.C's"* from *"Submarine chasers"*. They were quite resilient despite their wooden construction.

[8] *Ibid*.
[9] *Ibid*, f. 84.
[10] Norman Friedmann, *U.S. Small Combatants, including PT-boats, Subchasers, and the Brown-Water Navy: An Illustrated Design History*, Annapolis, Naval Institute Press, 1987, p. 27.

Over two hundred of them managed to cross the Atlantic during the war. Their greatest flaw was their small size which made life aboard difficult for the crews. The American Navy tried to adapt them for sea minesweeping operations, but with no success. As river sweepers however, they were well suited[11].

The US Navy contract was signed in April 1917, for 355 units to be delivered until January 1 1918. The figure was almost done, which allowed for the transfer of 50 ships to France. After 1 January, another 50 were sent to that country. Up until the end of the war the Americans build 441 of such ships, with 133 being transferred to allied countries[12]. In American services, they were used all over the Atlantic and Mediterranean theatres of operations, from England to the island of Corfu, in bases such as Otranto and Gibraltar. Some of them even escorted the transport ships in the Atlantic, from the Eastern coast to Bermuda, the most dangerous areas where the U-Boats prowled. In the Mediterranean, in conditions more close to the ones they would have faced in the Black Sea, the chasers would hunt in groups of three, detecting the enemy submarines with their hydrophones via triangulation. They would then use their depth charges to attack the U-Boats[13].

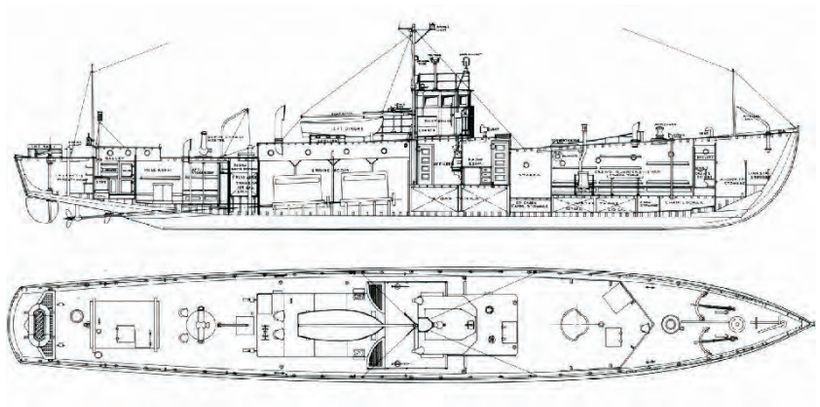

Photo 1: The design of the American S.C. ships[14]

[11] *Ibid*, p. 31.
[12] https://www.subchaser.org/statistics, retrieved on 16.04.2020.
[13] Norman Friedmann, *op. cit*., p. 32.
[14] Photo source: Norman Friedmann, *op.cit.*, p. 28.

The results of the investigation by the Romanian Naval Inspectorate on these ships were then sent to the War Ministry in Bucharest. They show a sense of urgency in the Romanian Navy in trying to get a hold of as many ships as they could, transitioning to a period of uneasy peace in the East. The limited strength of its naval forces was the main concern for the Inspectorate, especially as it expected a difficult situation on the Eastern borders of the countries as the tensions with Russia were soaring. The Navy was going through a period of transformation, as was the whole Romanian Army. This was expected to include the building up of its naval power in the Black Sea for its Sea Division there. In the Great War Romania tried to fight without a significant maritime force, relying instead on its allies, the Russians, to defend its coast. This was not possible in the future. The unification of Bessarabia also meant that it had to defend an even larger coast with the meager forces at its disposal.

The limited strength of its naval forces was the main concern for the Inspectorate, especially as it expected a difficult situation on the Eastern borders of the countries as the tensions with Russia were soaring. The Navy was going through a period of transformation, as was the whole Romanian Army.

This is why the report on the submarine chasers was very positive, the Chief of the Naval Inspectorate actually saying that *"this ship type would be very useful for us, not just in the current conditions, but in the future as well, whatever the organization of the Navy would be then"*[15]. Read Admiral Bălescu was referring to the process of reorganisation envisaged for the naval forces at the end of the war. The focus for the Navy then had to change from the Danube sector to the Black Sea region. In the first two years after the war, up until 1921, naval planners had to find new ways to change the structure of the Navy and circumvent the lack of funds available, even though they were insufficient even for the minimalistic projects.

As for the Black Sea Division, it was clearly going to be the emphasis for the Navy and most the resources were allocated for that sector. All of the naval analyses showed that the Navy could not fight *"with a hand tied on its back"*, as it did in 1916-1918, when Romania practically did not have any ships in the Black Sea and its coastal defenses were stripped.

[15] AMNR, Military Navy Command Collection, file 270, p. 84.

As many military analysts pointed out, the lack of investments in the equipment of the Sea Divisions was a major strategic mistake[16]. Confirming this, a report from the Chief of Staff of the Army to the War Ministry showed that the absence of Romanian naval power in the Black Sea led to a desperate situation there. After its allies retreated from the area and facing the Bolshevik threat, Romania was to contend to a communist fleet of three destroyers and two submarines in Odessa with practically no forces of its own[17]. Despite the fact that Russian fleet was not nearly as powerful as during the war or as it would become later on, it was still a significant threat. The Romanian Navy, on the other hand, had *"no means of securing its own coasts"* and could not stop the enemy from mining the seaways which meant that its communication with the Allied Powers could be severed at any time. The only solution that the General Staff saw going forward was to ask the Allied Naval Command to help the Romanian Navy by relinquishing no fewer than 4 1,000-ton destroyers, 12 submarine chasers and 12 hydroplanes[18]. The report also considered a backup solution, in the form of the gunboats that were being acquired from France[19], which could be pressed into service quite rapidly and used as minesweepers and coastal defense ships. This plan, to get ships from the Allies on a temporary or permanent basis was abandoned and the French gunboats with some *"M"* class destroyers would be the only maritime ships for Romania for a significant amount of time.

The only solution that the General Staff saw going forward was to ask the Allied Naval Command to help the Romanian Navy by relinquishing no fewer than 4 1,000-ton destroyers, 12 submarine chasers and 12 hydroplanes.

The submarine chasers inspected in 1919 seemed to help the Romanian Navy in a variety of ways; more than anything they would be a much needed military presence in the Black Sea. The Navy desperately wanted to have some sort of presence there, no matter what ship type would be involved. There were already reports about the submarine program that the Russians were developing, alongside

[16] Andreea Atanasiu-Croitoru, *"Forța navală maritimă a României între cele două războaie mondiale"*, in *Analele Dobrogei*, nr. X-XIII, 2009-2012, Muzeul de Istorie Națională și Arheologie Constanța, p. 72.

[17] AMNR, *5th Maritime Directorate*, file 386/1919-1920, f. 703.

[18] *Ibid*, p. 704.

[19] Andreea Atanasiu-Croitoru, *"Canoniera Locotenent comandor Eugen Stihi – o călătorie cât un centenar"* in Corneliu Postu, Petrișor Florea, Cornel Popescu (coord.), *Armata Română și Marea Unire*, studies and articles delivered during the National Scientific Papers Session, Pitești, 26 July 2018, Editura Militară, București, 2018, pp. 366-368.

other ships. In his report to the superiors in Bucharest, Rear Admiral Bălescu alluded to the Russian submarine threat when he spoke about the "threat from Russia". This was a danger for which the Romanian anti-submarine capabilities were inadequate to nonexistent[20].

Because the submarine chasers in question were of small size and had limited armaments, they were not very well suited to defend a large coastal area. The Navy concluded it needed a significant number of ships in order to organize many groups of ships. Their submarine detection capabilities were crude as well, given that at the time the hydrophones were a new development. Therefore, the Inspectorate argued for the creation of three squadrons, each with six ships. In turn, the squadrons would be divided into two groups of three hunters and placed in key areas of Drobrogea: Constanța, Sulina and Gura Chiliei[21]. With six ships in reserve, the total amount that the Romanians wanted to acquire was 24 units.

Their submarine detection capabilities were crude as well, given that at the time the hydrophones were a new development. Therefore, the Inspectorate argued for the creation of three squadrons, each with six ships. In turn, the squadrons would be divided into two groups of three hunters and placed in key areas of Drobrogea: Constanța, Sulina and Gura Chiliei.

Because it lacked other warships in the area, the Romanian Navy considered using the submarine chasers in a variety of other missions, not limited to anti-submarine warfare. The Navy had to defend a maritime coast of significant importance and had to rely on flexible ships, this meant that the submarine chasers had to patrol as well as fight enemy agents trying to infiltrate the coastline. The missions went as far as being able to be sent in *"information gathering incursions in enemy waters"*. This type of missions were very well suited for the submarine chasers, because they were very fast and their great speed could prove useful in evading enemy forces.[22]

There were other missions as well that the French ships of American origins would have had to do in the service of the Romanian Navy. These included transports of troops and materials along the Black Sea coast, even though the Naval Inspectorate acknowledged the fact that their small size would limit their capabilities for this type of tasks. They were also considering the possibility of using them in the role of achieving means of communication between land and sea forces, but the Inspectorate was more interesting in using the submarine

[20] AMNR, Military Navy Command Collection, file 270, p. 85.
[21] *Ibid*.
[22] *Ibid*.

chasers in peacetime. The ships could be employed as coastal patrols, a *"very precious mission in stopping the contraband"*[23]. In summary, the leadership of the Navy lobbied for the reception of 24 submarine chasers from France.

The series of interventions to the War Ministry to solve the crisis of lacking warships in the Black Sea continued with a new appeal from the Naval Directorate. This entity, under the Naval Inspectorate, also argued that the minefields in the Black Sea were threatening the navigation in the area. The problem was very serious and the fact that the Allied ships were retreating was making it worse. The unexploded mines could jeopardize the commercial ships sailing to and from Romanian waters. The Navy only had three improvised minesweepers, *"Basarab"*[24], *"Rareș"* and *"Ungheni"*, but they were riverboats and could not operate in the Black Sea. Although Romania had the obligation to sweep its own territorial waters, it just did not possess the means to do that[25].

ROMANIAN MILITARY THINKING

Alongside the negotiations for the "Frippone" gunboats (concluded with the acquisition of four units instead of the six the French offered), the Mission would offer different types of ships, especially motor boats, well suited for minesweeping. In August 1919, France started to pull back its naval forces from the Western coast of the Black Sea and from the Lower Danube area, expecting that this decision would force the Romanian Government to expedite the process of buying some of these very ships.

OTHER TYPES OF SHIPS OFFERED TO ROMANIA

Under these circumstances, the talks with the French Naval Mission would continue to reach new conclusions. Alongside the negotiations for the *"Frippone"* gunboats (concluded with the acquisition of four units instead of the six the French offered)[26], the Mission would offer different types of ships, especially motor boats, well suited for minesweeping. In August 1919, France started to pull back its naval forces from the Western coast of the Black Sea and from the Lower Danube area, expecting that this decision would force the Romanian Government to expedite the process of buying some of these very ships[27]. The Romanian Navy was aware of the French decision, because the representatives of the Naval Mission were open about it and went as far as expressing their conviction that *"given the complete lack of defence forces for the maritime coast"*, Romania would have

[23] *Ibid*, f. 86.
[24] A paddleboat, built in 1893 at the Naval Shipyards in Linz. During the war, it was part of the Minesweeping Group of the Romanian Navy. Georgeta Borandă, *op. cit*., p. 139.
[25] AMNR, Military Navy Command Collection, file 270, p. 69.
[26] For four million francs. Patrick Boureille, *op. cit*., p. 3.
[27] AMNR, Military Navy Command Collection, file 270, p. 87.

to resort to the French ships to *"create the nucleus of its naval force, which would, after a further expansion, ensure the hegemony of the Romanian flag in the Black Sea"*, as Lieutenant Commander Ioan Bălănescu, the Chief of the Naval Directorate, put it in his report[28]. Of course, we can safely assume that the Romanian Navy could not hope to achieve naval dominance in the Black Sea. This was not even the purpose of its existence, but the way in which the French officers chose to express their beliefs proves that they were employing a marketing strategy that was hoping to capitalise the Romanian natural fear of the Russian threat.

Captain O'Neill suggested that Romania should buy the gunboat "Decidee" of the "Surprise" class. These were colonial gunboats that had served during the war with good results. The ship that Romania would have bought served during 1914-1917 in the Indochina station. In the latter years of the war, it was part of the Syria patrol groups.

Even so, the French Naval Mission offered other alternatives for the development of the Romanian fleet, especially in regards to minesweepers. From the array of different ship types that were considered, two of them stand out because they were specifically built as minesweepers and not improvised: *"Gres"* and *"Marbre".* They were *"Granit"* class ships, launched in 1918, so a new design and build. Their characteristics were: displacement 360 t, length 58 m, breadth 8 m, draught 2 m. Their armament consisted of one 120 mm gun and another of 75 mm[29]. These minesweepers were inspected by Romanian Navy officials at Galatz with positive results. They were part of the French naval groups operating on the Danube and in the Black Sea.

Alongside the purposefully built minesweepers, the French Navy was ready to sell two ships of *"Herse"* class. An older design, from 1913/1914, the ships were called *"Rateau"* and *"Coquelicot"* and were smaller than the *"Granit"* ones. They displaced 255 t and were armed with 2x47 mm guns, but they were a cheaper alternative.

Also on the page of smaller ships, Captain O'Neill suggested that Romania should buy the gunboat *"Decidee"* of the *"Surprise"* class. These were colonial gunboats that had served during the war with good results. The ship that Romania would have bought served during 1914-1917 in the Indochina station. In the latter years of the war, it was part of the Syria patrol groups[30].

[28] *Ibid*.
[29] *Ibid*, f. 91.
[30] Robert Gardiner (coord.), *Conway´s all the World´s Fighting Ships 1906-1921*, London, Conway Maritime Press, 1985, p. 196.

Photo 2: The gunboat "Decidee"[31]

Its armament was considerable for a ship of her size: 2x100 mm guns, 4x65 ones and 1x37 mm. The displacement was 630 t and the crew was 100 men[32].

Captain O´Neill´s most spectacular idea was still to come. He argued that the Romanian Navy should buy at a lower cost the protected cruiser *"Jurien de la Graviere",* launched in 1899 and completed in 1903[33].

Captain O´Neill´s most spectacular idea was still to come. He argued that the Romanian Navy should buy at a lower cost the protected cruiser "Jurien de la Graviere", launched in 1899 and completed in 1903. This was an unsuccessful design of the French Navy, because it was poorly armed for a cruiser, with just 8 guns of 164 mm, 10x47 mm, 6x37 mm and two torpedo tubes of 450 mm.

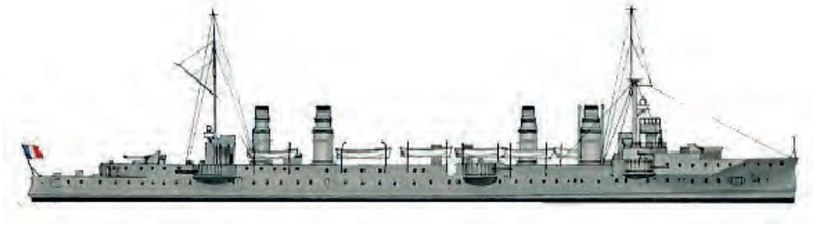

Photo 3: The cruiser "Jurien de la Graviere"[34]

This was an unsuccessful design of the French Navy, because it was poorly armed for a cruiser, with just 8 guns of 164 mm, 10x47 mm,

[31] Photo credit: http://servimg.com/image_preview.php?i=57&u=11930999#
[32] http://www.navypedia.org/ships/france/fr_of_surprise.htm, retrieved on 16.04.2020.
[33] Patrick Boureille, *op. cit*., p. 3.
[34] Photo credit: https://www.naval-encyclopedia.com/ww1/France/jurien-de-la-graviere/.

6x37 mm and two torpedo tubes of 450 mm[35]. The main artillery comprised eight Modèle 1893 164.7 mm guns, of which two were in shielded centerline mounts fore and aft, the remaining six in sides casemate mounts. The problems of the ship did not stop at the armaments. It was quite a slow ship, reaching 21 knots with some difficulty, even though the designed specified 23 knots. The engine compartment was cramped and she was extremely unhandy. It is no surprise then that, as with the other offers from the French, the cruiser was rejected by the Romanian Navy

CONCLUSIONS

After the end of World War I, France tried to ensure it had good relations in respect to the naval affairs of Romania, in so doing striving to use the strategic position of that country in Eastern Europe and in the Black Sea area. The volatile situation in Russia warranted some safety measures for the French. This meant keeping and actually expanding the naval mission in Bucharest in order to protect the lines of communication in the event of a military operation in the Russian Civil War. At the same time, the Naval Mission had to contend with the unexpected rivalry from the Royal Navy, who sent its own advisors in Romania.

Although it had the advantage of fighting together with the Romanians on the Danube and creating good relations with those allies, the French Naval Mission was experiencing difficulties consolidating its position in the Romanian Naval Inspectorate. The natural hesitations of the Romanian officers, some of the frictions during the war and other offers from different Western Powers, all contributed to a rather frustrating experience for the representatives of the French Navy.

Even so, the French naval officers tried to help the small Romanian Navy in its expansion process by offering different ships, some outdated, other of new designs, with which to create a naval force in the Black Sea.

[35] Fred T. Jane (coord.), *Jane´s Fighting Ships 1905/1906, A Reprint of the 1905/1906 Edition of Fighting Ships*, New York, Arco Publishing Company, 1970, p. 123.

BIBLIOGRAPHY

1. ***, Arhivele Militare Naționale Române/Romanian National Military Archives – AMNR, Military Navy Command Collection.
2. Patrick Boureille, *"Les relations navales franco-roumaines (1919-1928): les illusions perdues"*, in *Revue historique des armees*, 244/2006.
3. Andreea Atanasiu-Croitoru, *"Canoniera Locotenent comandor Eugen Stihi – o călătorie cât un centenar"* in Corneliu Postu, Petrișor Florea, Cornel Popescu (coord.), *Armata Română și Marea Unire*, studies and articles delivered during the National Scientific Papers Session, Pitești, 26 July 2018, Editura Militară, București, 2018.
4. Andreea Atanasiu-Croitoru, *"Forța navală maritimă a României între cele două războaie mondiale"*, in *Analele Dobrogei*, no. X-XIII, 2009-2012, Muzeul de Istorie Națională și Arheologie Constanța.
5. Norman Friedmann, *U.S. Small Combatants, including PT-boats, Subchasers, and the Brown-Water Navy: An Illustrated Design History*, Annapolis, Naval Institute Press, 1987.
6. Ion Ionescu, Georgeta Borandă, Marian Moșneagu, *Noi contribuții la istoria Marinei Militare Române*, Constanța, Editura Muntenia & Leda, 2001.
7. Robert Gardiner (coord.), *Conway's all the World's Fighting Ships 1906-1921*, London, Conway Maritime Press, 1985.
8. Fred T. Jane (coord.), *Jane's Fighting Ships 1905/1906*, *A Reprint of the 1905/1906 Edition of Fighting Ships*, New York, Arco Publishing Company, 1970.

WEBOGRAPHY:

1. www.naval-encyclopedia.com.
2. www.subchaser.org.
3. www.navypedia.org.

Președintele României

Dorind a răsplăti meritele

revistei

„Gândirea militară românească"

cu ocazia împlinirii a 110 de ani de existență, pentru rezultatele deosebite obținute în întemeierea doctrinei și concepției 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/ nr. Cat, 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 Ier. 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