ROMANIAN MILITARY THINKING

romania2019.eu

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

2/2019

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

Printed
at Military Technical Publishing Centre
C ___/2019 B 0207

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

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 XV –

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

On 6-7 November 2019,
the Defence Staff will organise
the conference
Security and Defence between History, Theory and Public Policies,
in the context of the 160th anniversary of the Defence Staff
and the 155th anniversary of Gândirea Militară Românească Journal.

Conference main purpose:

Debate on the issue of national security and defence, in the context of the latest developments of the regional and global security environment.

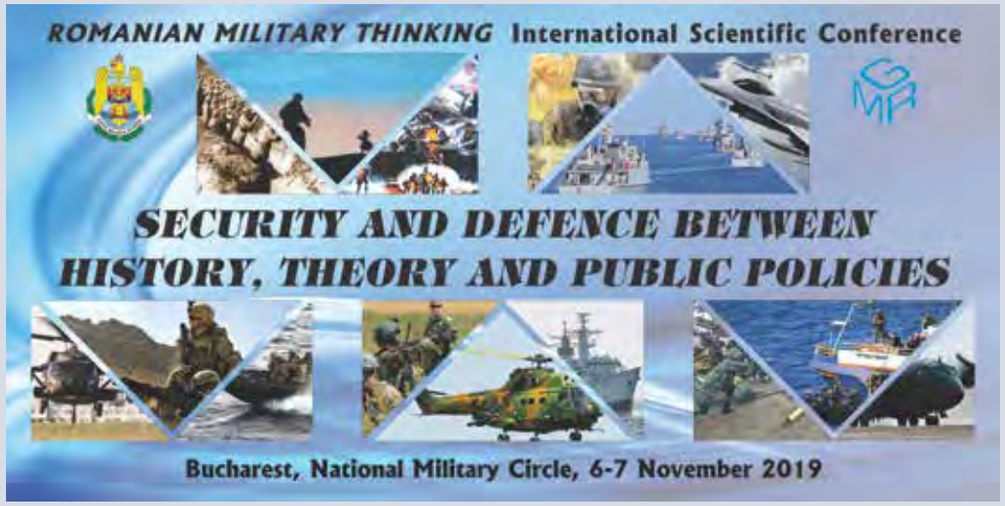
An author may participate with a maximum of two papers, signed individually or as co-author. A paper can have up to 3 co-authors.

The papers will be peer-reviewed by an international scientific committee. Conference papers will be published in a volume with ISSN code, in English, both in print and electronically (limited edition, for academic libraries).

Only papers that are submitted before the deadline and pass the scientific evaluation will be published. The best rated papers will be published in a special bilingual issue (Romanian and English) of the Gândirea Militară Românească Journal (indexed by EBSCO database)

Contributors:

The following are expected to participate in this activity: representatives of military services, NDU, military academies, Defence Staff, Romanian collaborators of Gândirea Militară Românească Journal, military academies' professors and students/Master's students/PhD candidates, military researchers, specialists, experts, academic staff and researchers from Romanian civil education and research institutions, representatives of the Presidential Administration, EURISC (European Institute for Risk, Security and Communication Management) Foundation, ESGA (Expert for Security and Global Affairs) Association, Monitorul Apărării, New Strategy Center, Ministry of Internal Affairs (Romanian Police, Romanian Border Police, Romanian Gendarmerie, General Inspectorate for Emergency Situations), Ministry of Foreign Affairs (Operational Centre for Emergency Situations), Romanian Intelligence Service, specialists and experts from other institutions belonging to the National system of defence, public order and national security, students, Master's students, PhD candidates.



CONFERENCE SECTIONS

MILITARY THEORY AND ART

Contemporary military phenomenon: challenges and trends

This section seeks to point out the complex interaction between theory and practice in the military field, by reffering to the main concept and technologies leading to the evolution of military strategy throughout history.

INTELLIGENCE AND SECURITY

Innovation, the main driver of change in the field of security and defence

The relation between intelligence and the concept of (national and international) security is meant to explain and promote common defence policies, generated following the decisions taken during the NATO Summits of the last decade and at the European Union level. A new arms race, asymmetric threats, cyber security or impact of artificial intelligence on security are only a few of the aspects that have led to reviewing the priorities of international actors, in the field of security and defence.

DEFENCE RESOURCES MANAGEMENT

Smart Defence: from initiative to operational concept

The pace of change and transformation involved by the new revolution in military affairs has increased lately, especially in the aftermath of the September 11, 2001, attacks. Although the essence of war has not changed, the forms and procedures of military action, armed fight included, have evolved, depending on the features of the strategic security environment, forces, means, weapon systems, policies and strategies.

MILITARY HISTORY

The evolution of Romanian Military Thinking in the past 160 years

In terms of strategic thinking, things are uncertain these days. A set of questions can become rather enlightening for a solid foundation in knowledge. Is there still a dominant school of military thinking at world level? Is the new paradigm of strategic and military thinking actually a return to the old paradigm? Are there reasons to believe in the Clausewitzian war, in which the principles of the Prussian General can still prove their efficiency? These questions continue to remain unanswered in a world in which the role of the state continues to be important.

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)

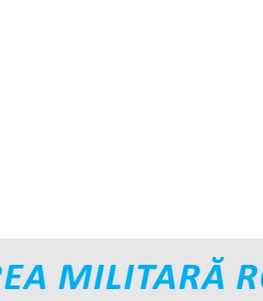
[1] *Din trecutul României Militare cu prilejul aniversării a 75 de ani de la apariția ei în viața armatei. 1864-1939*, București, 1939, p. 31.
[2] *Ibidem*, p. 32.
[3] *România Militară*, no. 1, 1981, p. 6.

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

"Division General Ștefan Fălcoianu" Award



"Lieutenant Colonel Mircea Tomescu" Award

"Army Corps General Ioan Sichitiu" Award

"Marshal Alexandru Averescu" Award

CONTENTS

ON HYBRID WARFARE AND COUNTERING ITS EFFECTS

Brigadier General Marian BOTEA

Chief of Operations Directorate, Defence Staff

English version by **Iulia SINGER**.

The global security environment is currently experiencing a dynamic of change that has been more intense than ever in the past decades. There is a tension of international relations on all the axes of geopolitics, tension amplified by communication and media globalisation, by the perpetual threat posed by terrorism, as well as by the difficulty of delimiting the classic risks from the asymmetric or hybrid ones. The fact that older or newer, state or non-state actors bring back on the international stage glossed-over interpretations of force policies only complicates things.

It is almost impossible to associate the notion of predictability with this state of affairs. As for the effects of these twisted international relations, it can be stated with certainty only that they will continue to deepen instability at the global level, an instability that is becoming more easily transformed into aggression by interested actors. And the "weapon of choice" of the latter seems to be hybrid warfare, in its various versions.

Essentially, although the physiognomy of the war has changed, tailoring itself, from the tactical point of view, to meet the features of the historical period in which it broke out, it essentially remained purely Clausewitzian, in the sense that it remains an instrument of politics. As for its "hybrid" dimension, so debated in the last decade within the defence and security community, it is not an absolute novelty, in our opinion. For countless times throughout history the weaker opponent has tried to identify and fully exploit the vulnerabilities of their stronger opponent and has often done so without considering rules, norms or tactics strengthened and practiced beforehand. From this point of view, the hybrid feature of warfare is just one of its many extensions, together with the guerrilla, we could say, although not even the Iberian guerrilleros, who so very courageously opposed Napoleon, can be labelled as the promoters of the hybrid version of war.

The concept of hybrid warfare does not have a generally accepted definition. An attempt to define it should necessarily include a list, one that is not intended to be exhaustive, highlighting its main features, namely: hybrid warfare uses a multitude of means, military, but especially non-military ones, such as economic, diplomatic, information ones, all of which are, in fact,

within the range of the instruments of state power; the instruments usually act in concert, in order to maximise the effects and to achieve the obvious strategic goals that seek the total unbalance of the enemy's decision-making capacity; the intensity of the action is kept below a certain threshold, above which it could be assimilated to an open conflict; the ambiguity and denial of involvement are a compulsory part of the arsenal, with the aim of concealing the hybrid action up to making it untraceable in time and space. If we also add its main effects – to destabilise the state, to polarise the society and to disturb the enemy's defence system –, we will get a rather suggestive picture of this type of conflict which, according to many specialists, has not yet reached the upper limit of development.

The danger posed by hybrid threats is rising. The speed of development of the new technologies and the speed at which the society is today engulfed in unfiltered information make possible the manifestation of the effects of this type of conflict, whose purpose is to gain the victory by destroying the target without launching a classic military attack. Therefore, although the concept implies the predominant use of non-military means, the military factor still plays a very important role, being the supreme instrument of pressure and deterrence. If the target state has massed on its border a few enemy tank divisions, the ability to resist and attempt to respond is seriously compromised.

After the annexation of Crimea, in 2014, many military analysts rushed to declare that this new way of conducting the war was invincible and that it could be projected anywhere in the world, the evidence being the alleged involvement in the voting processes in the US and in other European countries. The truth is, however, that this type of conflict also has limitations and the initiator certainly has their own vulnerabilities, which could be exploited by an effective countering and discouragement strategy. The main challenge is to identify the attack, which should happen from the preliminary stages, in order to be effective. This is almost impossible to achieve. However, there are other aspects, which are essential in defining a response to hybrid threats: to organise a functional and flexible cyber defence, to ensure an efficient communication system even in the most critical situations, to achieve a response system at the level of strategic communications so that the magnitude of the effects of destabilising propaganda and fake news is as low as possible, to implement a warning system capable of quantifying and transforming the entire range of hybrid risks into early warning indices. A key role is played

by the need for increasing societal resilience, starting from the state's ability to function even in the event of serious crises, ensuring the necessary resource flows and focusing on public awareness, as the latter is most exposed to hostile subversive activities. In fact, here is one of the sticking points of any anti-hybrid strategy, in a democratic society: the state cannot take all the measures required to guarantee the complete safety against these threats without finding itself, at one point, in the potential danger of being accused of dictatorial behaviour and attack on fundamental freedoms.

With regard to the classic concept of "deterence", the doctrinal basis of the Cold War, which, in fact, proved to be functional, ensuring the necessary balance to avoid a catastrophic conflict, the question arises whether it can regulate the situation in the case of hybrid threats. The answer tends to be positive, although the debate is still ongoing. Indeed, we must agree that there are threats that cannot be eliminated, when the limits of the democratic state intervene. A totalitarian state has at its disposal the tools of force meant to ensure, even temporarily, the total unity of action.

Currently, the book of lessons learned in this area remains open. There are many aspects to study and assimilate about the techniques, tactics and procedures of hybrid warfare, considering that its different forms will make their presence felt in the inherent conflicts of the future. Yet, as long as the costs of doing thus will be too high or the rewards too low, those who will want to use this new form of aggression will need to seriously calculate the risks they will face in the long run. And, as a conclusion at this stage, in the end, as in any escalation, the resources are the ones that win the race.

HYBRID WARFARE AND ITS MANIFESTATIONS IN THE CRISIS IN UKRAINE

Lieutenant Colonel Mihai-Cristian STANCU

Advanced Instructor, Land Forces Department,
Command and Staff Faculty,
PhD student, "CAROL I" National Defence University

The form of war that Russia admitted to using in Crimea and tried to use in Ukraine, too, came to be known as "hybrid warfare". This phrase has already been included in numerous articles, papers and news reports**, and after the summit in September 2014 in Wales, the concept of hybrid warfare was adopted by NATO. It is also noteworthy that this phrase originally had a different meaning, and clarifying the issues of semantic thinking requires a brief resort to history to study the origin of the concept and its later development.*

This scientific article will be completed by using a few of the analysis and research methods specific to sociology, but very well fitted to the military science domain. Through the method of data collection, which is an empirical one, we will analyse the meaning of hybrid warfare in Western and Russian doctrines and its manifestations in the crisis in Ukraine. Furthermore, we will watch the hybrid warfare evolution using the historic method from the very beginning, when William J. Nemeth mentioned for the first time this phrase, to Gerasimov's non-linear concept. The balance that we will thus achieve between the theoretical elements of the hybrid warfare and the way the Ukraine crisis developed will demonstrate that this conflict was a hybrid one within all its components. By using the analysis method, we have managed to develop this article and its argumentative support.

Keywords: hybrid warfare, armed fight, field operational art, Ukraine, guerrilla techniques.

* Andras RACZ, *Russia's Hybrid War in Ukraine*, The Finnish Institute of International Affairs, p. 27.
** At 12.09.2016, Google showed 132.900 "responses" for "hybrid warfare".

romania2019.eu

Introduction

The nature of conflicts throughout modern history of mankind has evolved through the remarkable changes that have taken place in society. Until after the Second World War, winning a war would have involved massive armies, strongly supported by artillery fire and air strikes, concentrated in a coordinated manoeuvre of forces and means. With the proliferation of terrorism, the conduct of the conflict has taken on other meanings, caused mainly by changes in contemporary society. It has been proved in recent conflicts that insurgency and terrorist organisations are able to defeat opponents that are more powerful, equipped with modern technology and superior in number. The security establishment has met new challenges starting with the outbreak of the crisis in Ukraine, where the West was confronted with a fait accompli. *"The new generation of war"* of the Russian Federation, as Chief of General Staff General Valery Gerasimov called it, surprised both the targeted state, Ukraine, and the international environment by the speed, adaptability to confrontation environment, prove ingenuity, and especially by the highly effective coordination of military capabilities with non-military means. That has surprised the decision-makers from state and non-state actors (NATO, EU, OSCE etc.) and the broad scope of event actions closely-knit between military and non-military levels sparked concern in the international environment due to the typology of the conflict, its size and the lack of means to prevent and counter such hostilities. Given the ambiguity of the actions and its comprehensive nature of expression, Western experts have called this manifestation of conflict as *"hybrid warfare"*, updating some theories of the 21st century to the current issues encountered in the Ukrainian crisis.

With the proliferation of terrorism, the conduct of the conflict has taken on other meanings, caused mainly by changes in contemporary society. It has been proved in recent conflicts that insurgency and terrorist organisations are able to defeat opponents that are more powerful, equipped with modern technology and superior in number.

The emergence of the hybrid warfare concept

Thus, the term *"hybrid warfare"* was used for the first time in Major William J. Nemeth's paper, written in 2002, at the Naval School in Monterey, USA, entitled *"Future War and Chechnya: A Case*

ROMANIAN MILITARY THINKING

of Hybrid Warfare"[1] . Nemeth said that Chechen society was at that time in a *"hybrid situation"*, evidenced by the fact that the contemporary state had the societal architecture built in traditional style – made up of clans and families. This structural typology allowed the Chechens to mobilise the society for war and to support armed resistance through linked clans and family relationships, something which proved successful against the Russians. What is relevant from the perspective of this paper is that this type of hybrid society developed a hybrid way of waging armed struggle, which combined elements of conventional and irregular warfare in an effective and flexible manner. Besides a detailed knowledge of the land and the generous support due to relations and kinship within the clan, Chechens successfully combined elements of Western and Soviet military doctrine with guerrilla tactics and the use of modern technology. Chechen's Battle Mode was characterised by flexibility, allowing alternate guerrilla tactics engagement with conventional Russian forces tactics, depending on their manoeuvres. Also, knowledge of Russian language and Russian culture facilitated the planning and execution by Chechen forces of extensive and effective psychological and information operations, which succeeded in undermining both Russian military morale and attracting political support from the West. Thus, the defining element of the Chechen war was its *"comprehensive nature"*[2], because it involved the whole society. Thus, we can say that within hybrid warfare, there is a blurred distinction between *"combatant"* and *"non-combatant"* and the phenomenon of terrorism, massacres and inhumane treatment of prisoners of war may appear to achieve the desired end state. In conclusion, the term *"hybrid warfare"* in the work of Nemeth highlighted a type of warfare specific for the society that combined conventional and irregular tactical elements with contemporary information tools and procedures. Nemeth's theories were developed later (2008) by John McCuen in the article which appeared in *"Military Review"*[3] stating that hybrid warfare is waged on three decisive fronts: the first being the conventional one in which the attacked state's armed forces face both conventional and asymmetric (irregular) threats;

The defining element of the Chechen war was its "comprehensive nature", because it involved the whole society. Thus, we can say that within hybrid warfare, there is a blurred distinction between "combatant" and "non-combatant" and the phenomenon of terrorism, massacres and inhumane treatment of prisoners of war may appear to achieve the desired end state.

[1] Andras RACZ, *op. cit.*, p. 28.
[2] *Ibid*, p. 28.
[3] J.J. McCuen, *"Hybrid Wars"*, in *Military Review*, March-April 2008, available at http://au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf, retrieved on 13.09.2018.

the second front being the local population of the attacked state, that is to be controlled and convinced of the intentions of the attacker; while the third front is made up of the civilian population of the attacking state and the international community, whose support is essential, especially in long, attrition conflicts.

In this context, F. Hoffmann showed that hybrid threats encompass a broad spectrum of ways of waging armed struggle (conventional manoeuvres, irregular tactics, terrorist acts, massacres etc.) that may be carried out by both state and non-state actors[4]. Furthermore, the author emphasises that these multimodal actions may be conducted by separate units or the same unit, directed and coordinated in the area of confrontation to achieve synergic effects within the physical and psychological dimensions of conflicts at all three levels of operation – tactical, operational and strategic[5]. Therefore, it can be stated that the efficiency of hybrid warfare is given by convergence and coordination, enabling stakeholders to work together to achieve a common result, as well as the destructive potential, in perpetual development, of the modern weapons systems. However, it is worth noting that conventional threats should not be neglected in the process of developing defence strategies. The emergence of hybrid warfare does not mean that conventional warfare is irrelevant or obsolete, but rather reflects a new level of threat that modern armed forces must be able to counteract.

According to F. Hoffman, *"hybrid warfare encompasses a wide range of different types of warfare, including conventional capabilities, irregular/asymmetric formations and tactics, terrorist violence and coercion, and criminal unrest"*[6]. The definition given by F. Hoffman is also used by Petri Huovinen, who describes hybrid war as *"a cocktail of conventional military capabilities, insurgency, terrorism, guerrilla warfare, organised crime, cyber warfare and advanced military technology"*[7].

romania2019.eu

The efficiency of hybrid warfare is given by convergence and coordination, enabling stakeholders to work together to achieve a common result, as well as the destructive potential, in perpetual development, of the modern weapons systems. However, it is worth noting that conventional threats should not be neglected in the process of developing defence strategies. The emergence of hybrid warfare does not mean that conventional warfare is irrelevant or obsolete, but rather reflects a new level of threat that modern armed forces must be able to counteract.

[4] F.G. Hoffmann, *"Conflict in the 21st Century: The Rise of Hybrid Wars"*, Potomac Institute for Policy Studies, Arlington, Virginia, December 2007, p. 8.
[5] *Ibid*.
[6] *Ibid*.
[7] Petri Huovinen, *"Hybrid Warfare – Just a Twist of Compound Warfare"*, National Defense University, 2011, p. 7, available at https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf, accessed 13.09.2018.

ROMANIAN MILITARY THINKING

Considering the approaches above and the conduct of recent conflicts on the international arena, it is considered that the hybrid warfare can be characterised as a conflict in which one side, through careful organisation and coordination, uses a combination of conventional and unconventional capabilities, in order to create a wide range of threats to capture and dissipate the opponent's efforts and make it impossible for the opponent to make appropriate use of conventional forces and means[8].

In most cases, the specialised literature does not make a clear distinction between the hybrid warfare and the conflict of hybrid nature. Hybrid conflict can be defined as a crisis situation with a broad spectrum that includes both the physical and the conceptual dimensions: the first is the fight against an armed enemy and the other is the complex fighting for gaining the support of indigenous people in conflict areas, the public support of the states contributing to the operation and the support of the international community.

In most cases, the specialised literature does not make a clear distinction between the hybrid warfare and the conflict of hybrid nature. Hybrid conflict can be defined as a crisis situation with a broad spectrum that includes both the physical and the conceptual dimensions: the first is the fight against an armed enemy and the other is the complex fighting for gaining the support of indigenous people in conflict areas, the public support of the states contributing to the operation and the support of the international community[9].

Hybrid warfare involves the simultaneous employment of conventional and unconventional forces in carrying out the fight and the permanent adaptation of political, military, economic, social, information or diplomatic means for reaching the political and military goals set[10].

Hybrid Warfare in Western and Russian understanding of the concept

The changing nature of conflicts and the emergence of new forms of waging armed struggle have raised issues for study both in the West and in Russia. The new generation of war presents different shades for the two actors, and a comparison between the American and Russian thinking is appropriate in order to define their approach to hybrid warfare.

Since 2009, the US Joint Forces Command adopted a *"semi-official"* definition of hybrid threats, during a conference in Washington. Thus, hybrid threat is defined as *"any opponent who simultaneously and flexibly engages, in the space for confrontation, an adapted combination of conventional, irregular, terrorist and criminal resources and activities. Hybrid threat is more than one entity and comprises a combination of state and non-state actors"*[11]. It should be emphasised that the definition above focuses only on the use of force and violence, not considering the use of political, diplomatic and economic instruments.

[8] Col. Liviu Ioniță, *Physiognomy of Contemporary Conflicts. The Rise of Non-linear Approaches*, p. 23.
[9] *Ibid*, p. 24.
[10] *Ibid*.

romania2019.eu

Also in 2009, during a US-Israeli working group regarding issues of *"War gaming"* about hybrid threats, American expert Richard Glenn defined the hybrid threat as *"an opponent who simultaneously and flexibly employs some combination of (1) political, economic, social, and information instruments and (2) conventional, irregular/asymmetric, catastrophic, terrorist and criminal methods of waging armed struggle. It may include a combination of state and non-state actors"*[12]. This aspect of novelty brought by Glenn is taking in consideration the use of non-violent instruments of the political economic, social and information spectra. Thus, one can notice a remarkable similarity between Glenn's definition and the events in Crimea and eastern Ukraine. In the spring and summer of 2014, Russian armed forces and pro-Russian separatists used most of the instruments and methods mentioned by the American expert. The only exception (at least for now) is the catastrophic terrorism or the major disasters that could have caused extreme damage to the population, the natural environment, infrastructure and functioning of central and local administrations.

Since 2009, the US Joint Forces Command adopted a "semi-official" definition of hybrid threats, during a conference in Washington. Thus, hybrid threat is defined as "any opponent who simultaneously and flexibly engages, in the space for confrontation, an adapted combination of conventional, irregular, terrorist and criminal resources and activities. Hybrid threat is more than one entity and comprises a combination of state and non-state actors".

Yet, Glenn's definition was not accepted in all US media of research regarding this phenomenon. In 2012, Williamson Murray and Peter R. Mansoor published a collection of essays on hybrid warfare, which defined the concept as *"a conflict that involves a combination of conventional military forces and irregular forces (guerrillas, insurgents and terrorists), and may include both state and non-state actors, planned in order to achieve a common political objective"*[13]. It is to be underlined that the authors perceive and describe hybrid warfare actions focusing on military and irregular armed forces' actions, looking less at the social and information aspects.

[11] R. Glenn, *Thoughts of Hybrid Conflict*, in *Small Wars Journal*, 2 March 2009, available online at http://smallwarsjournal.com/mag/docs-temp/188-glen.pdf, retrieved on 13.09.2016.
[12] *Ibid*.
[13] M. Williamson-P. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, Cambridge, 2012, p. 321.

ROMANIAN MILITARY THINKING

NATO first used the term *"hybrid warfare"* on 3 July 2014, in a video on the security situation in Eastern Europe. Subsequently, the North Atlantic Treaty Organization adopted this term during the summit in Wales (September 2014) describing hybrid warfare as *"a wide range of military, paramilitary and civilian covert or open actions [...] engaged in a highly integrated design"*[14]. The fact that NATO adopted the term *"hybrid warfare"* contributed to the widespread use of this concept instead of others such as *"non-linear warfare"*, *"indirect warfare"* or *"full spectrum conflict",* formulated by other experts. Although this phrase is widely accepted in NATO and partner countries, one should also consider its development in time, as it has happened since 2002 (when it was first used by J. Nemeth) until now. Initially, Nemeth characterised hybrid warfare as a flexible form of fighting, combining elements of conventional tactics and irregular elements (Russian-Chechen conflict 1994-1996), so that to evolve to a form of combined fighting, comprising conventional capabilities, irregular tactics and formations, and terrorist violence (F. G. Hoffmann), and now become the preferred term to describe conflicts in Crimea and eastern Ukraine.

NATO first used the term "hybrid warfare" on 3 July 2014, in a video on the security situation in Eastern Europe. Subsequently, the North Atlantic Treaty Organization adopted this term during the summit in Wales (September 2014) describing hybrid warfare as "a wide range of military, paramilitary and civilian covert or open actions [...] engaged in a highly integrated design".

In terms of Russian military thinking, in 2013, Chief of General Staff of the Russian Armed Forces, General Valery Gerasimov, characterised contemporary warfare as *"the new generation of warfare"*[15]. Based on the events of the *"Arab Spring"*, Gerasimov referred to the new generation of warfare as *"the combined use of (1) diplomatic, economic, political and other non-military instruments with (2) direct military intervention"*[16]. He insisted that the rules of war had changed, arguing that the role of non-military means to achieve political and strategic objectives grew, often being more effective than conventional forces. Gerasimov expected a veiled use of force, through paramilitary or insurgent groups that were to act asymmetrically.

He also noted that, apart from the physical dimension, contemporary wars must necessarily include the information space. In developing his ideas, he insisted on the execution of surgical strikes (carried out by strategic aviation or even through satellite) in the depth of enemy territory to destroy civilian and military infrastructure in a short amount of time. Moreover, he supported the substantial

[14] *Ibid*.
[15] Andras RACZ, *op. cit.*, p. 36.
[16] *Ibid*.

use of special operations forces and robotic arms (e. g. drones), followed by the involvement of regular forces only in the final stages of the conflict, most of the time dissimulated in forces for peacekeeping or crisis management. It should be mentioned that the Russian strategists call it the *"non-linear war"*[17] or *"special war"* in order to make a clear difference between their concept and the Western concept of hybrid warfare. This non-linear war is an extension of Russia's guerrilla geopolitics specific to the last two decades.

In the February 2013 issue of Russian journal *"Military Industrial Kurier"*, Gerasimov emphasised that the wars of the 21st century woukld not make a clear distinction between the state of war and peace, referring to them as *"undeclared wars"* – *"wars will no longer be declared and once started they will continue in an unprecedented format"*. According to his theory, Russia's strategy of future warfare will not be based on traditional military methods, according to which military actions follow strategic deployments and declarations of war (regulated by the Vienna Declaration, 1896). Consequently, upfront confrontations executed under strict military hierarchy, based on firepower and significant human resources, will be replaced by non-contact *"clashes"* between very mobile units, *"military actions in peacetime"* carried out by *"armed civilians"*, which will require an adequate system of force management in a common information area[18].

Sergei Chekinov and Sergei Bogdanov[19] elaborated on Gerasimov's theory, producing a more detailed analysis of the *"new generation of warfare"*. They stated that the first *"new generation"* war in history was the Gulf War, which was analysed to highlight the distinctive features of the new form of waging armed struggle. In general, the authors supported Gerasimov's theory, emphasising the importance of asymmetric actions for neutralising military superiority of the enemy by the combined use of political, economic, technological and information instruments. According to the authors, the *"new*

romania2019.eu

Sergei Chekinov and Sergei Bogdanov elaborated on Gerasimov's theory, producing a more detailed analysis of the "new generation of warfare". They stated that the first "new generation" war in history was the Gulf War, which was analysed to highlight the distinctive features of the new form of waging armed struggle. In general, the authors supported Gerasimov's theory, emphasising the importance of asymmetric actions for neutralising military superiority of the enemy by the combined use of political, economic, technological and information instruments.

[17] M. Galleotti, *The 'Gerasimov Doctrine' and Russian Non-Linear War,* available at http://cs.brown.edu/people/jsavage/VotingProject/2017_03_09_MoscowsShadow_GerasimovDoctrineAndRussianNon-LinearWar.pdf, retrieved on 17.05.2019.
[18] J. Berzins, *Russia's New Generation Warfare in Ukraine: Implication for Latvian Defence Forces*, National Defence Academy of Latvia, Center for Security and Strategic Research, 2014, p. 4.
[19] S. Chekinov, S. Bogdanov, *The Nature and Content of a New Generation War*, *Military Thought*, October-December 2013, pp. 12-23.

generation of warfare" will be dominated by clashes in the information and psychological areas, aiming to weaken the morale of the troops and of the civilian population in order to erode *"their will to resist"*[20]. In addition, they also anticipated the proliferation of non-traditional means of fighting the wars of the future, such as weapons capable of influencing weather conditions or earthquakes, and the use of robotic arms or autonomous weapons systems. Finally, Chekinov and Bogdanov concluded that wars of the *"new generation"* will be divided into two phases[21]: the opening of the conflict and its termination. The opening phase will begin with a non-military campaign against the target state, extremely intense and extended over several months, which will include diplomatic, economic, ideological, psychological and information measures. To these a powerful propaganda campaign is added to deter people, increase their lack of satisfaction with the central authorities and weaken the morale of the armed forces. Blackmail and bribery of government and military officials will also be carried out to influence the function, alerting and mobilisation of enemy armed forces. In addition, the attacker will infiltrate undercover agents who will carry weapons, funding and other materials sufficient for committing terrorist attacks, orchestrating challenges and generating situations of chaos and instability.

Chekinov and Bogdanov concluded that wars of the "new generation" will be divided into two phases: the opening of the conflict and its termination. The opening phase will begin with a non-military campaign against the target state, extremely intense and extended over several months, which will include diplomatic, economic, ideological, psychological and information measures.

Furthermore, prior to military engagement, reconnaissance and subversion missions will be carried out, using a variety of means and methods of gathering information, ranging from diplomatic missions to espionage, so as to identify and locate military units, significant government offices and major infrastructure works. These are followed by triggering large electronic warfare operations, accompanied by cyber-attacks designed to prevent the functioning of government and military institutions.

Soon the military intervention occurs, probably starting by a vast air attack that will include strategic airstrikes, precision ballistic missiles, drones, long-range reactive artillery systems and other automatic weapons. According to the authors, at the end of the opening phase of the conflict, the central political-military institutions of the enemy

[20] *Ibid*, p. 16.
[21] *Ibid*, pp. 19-20.

state will find themselves unable to work, something that will cause confusion and a real mess in the deployment of armed forces.

The closing phase of the *"new generation warfare"* is represented by the attack carried out by conventional forces in order to destroy and/or isolate points of resistance that have *"survived"* the initial phase. Some Western interpretations of Gerasimov theory (see Mark Galeotti – expert analyst of Russian security services) claim that the Russian General used "defensive exposure" in developing its vision of characterising *"the new generation of warfare"*. Thus, Galeotti noted that Gerasimov concealed his true intentions by using reverse psychology, referring to the need to defend Russia against Western threats, having as an origin the *"new generation of warfare orchestrated by the USA in the Arab world"*. Through the need to defend Russia against a potential war similar to that orchestrated by the West in the Arab world, Gerasimov wanted to emphasise exactly the opposite, namely that this is the kind of war that must be developed by Russia[22].

The closing phase of the "new generation warfare" is represented by the attack carried out by conventional forces in order to destroy and/or isolate points of resistance that have "survived" the initial phase. Some Western interpretations of Gerasimov theory (see Mark Galeotti – expert analyst of Russian security services) claim that the Russian General used "defensive exposure" in developing its vision of characterising "the new generation of warfare".

Within the Russian paradigm of *"hybrid warfare"* management, taking advantage of the Russian political system that can fully subordinate the media capabilities to exploit energy resources, security and intelligence systems, as well as conventional military forces in achieving the political goal set, the main direction of action is gaining access, insertion or interference in/with decision-making processes of both partner countries and especially of the opponents to influence/alter them thereof. The approach is based on the theory of *"controlling reactions"*, according to which the enemy must be subject to an intense *"information/disinformation attack"* designed to voluntarily trigger a certain reaction, desirable for Russian initiators. At the limit, identifying the pattern of thought, decision and execution of the enemy in order to identify vulnerabilities in these processes, its *"big picture"* or the premises envisaged are considered the highest form of knowledge of the opponent. By acquiring knowledge about the processes of decision-making and execution models, Russian policymakers are able to start engaging their opponents in an integrated manner, using: kinetic, information, economic and energy policy and influence actions.

[22] M. Galeotti, "*The Gherasimov Doctrine and Russian Non-Linear War*", 6 July 2014, available online at htpps://inmoscowshadows.wordpress.com/2014/07/06the-gherasimov-doctrine-and-russian-non-linear-war/, retrieved on 16.09.2018.

ROMANIAN MILITARY THINKING

Specific aspects of the concept of hybrid warfare during Russian Federation's intervention in Ukraine

The Russian military intervention in Ukraine was caused by Moscow's perceptions about the geopolitical and socio-political threats derived from Kiev's getting out of its sphere of influence and control. The complexity of these perceptions is also reflected in the hybrid manner of action, a manner adjusted to the aims followed and common to interventions both in Crimea and eastern Ukraine, where Russia's hybrid action was based on five fundamental principles of general applicability, even if the situation in the field can generate further developments.

The Russian military intervention in Ukraine was caused by Moscow's perceptions about the geopolitical and socio-political threats derived from Kiev's getting out of its sphere of influence and control. The complexity of these perceptions is also reflected in the hybrid manner of action, a manner adjusted to the aims followed and common to interventions both in Crimea and eastern Ukraine, where Russia's hybrid action was based on five fundamental principles[23] of general applicability, even if the situation in the field can generate further developments.

Underlying Russian intervention in Ukraine and not only (see Georgia, Czechoslovakia), we find the *"Po Zakonu"* concept, meaning in accordance with the law. Russian diplomatic and information campaign showed Moscow's actions in Ukraine as being apparently legal or in a grey area of international law that are generally accepted, an area where previous different interpretations represent a precedent, and the precedent of Western intervention in Kosovo was used extensively. From a strictly military point of view, two concepts were used in tandem. First, deterrence by punishment[24], deterrence through the threat of retaliation, in which enemy action is paralysed because of the fear of massive retaliation. In the case of annexation of Crimea, Kiev decisional paralysis was caused by the massive concentration of Russian troops at the border. In the case of separatist insurgency in eastern Ukraine, Kiev understood in August 2014 that any large-scale operation against separatists would cause direct intervention, albeit limited, of the Russian army, in order to even out the balance of forces on the ground. The second military concept, that of denying the intervention by using special forces under cover, was materialised by the presence of *"little green men"* in Crimea and *"volunteers"* in eastern Ukraine.

[23] Douglas Mastriano, *Defeating Putin's Strategy of Ambiguity*, blog post *War on the Rocks*, available at http://warontherocks.com/2014/11/defeating-putins-strategy-of-ambiguity, retrieved on 8.09.2018.

[24] *About the Concept of Deterrence through the Threat of Retaliation, see* Michael S. GERSON, *Conventional Deterrence in the Second Nuclear Age*, Army Strategic Studies Institute, 2009, pp. 40-42, available at http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/09autumn/gerson.pdf, retrieved on 24.01.2019.

romania2019.eu

If we make an inductive analysis of Russian operations conducted in Ukraine, it can be considered that hybrid warfare consists of three phases, each of which in turn comprises three stages[25], as follows:

1. *The preparatory phase* was to identify strategic, political, economic, social and infrastructure vulnerabilities of the target state and set the appropriate means for their exploitation. In the case of Ukraine, Russia was favoured in this respect, given their common history, close economic and social ties and close relations between political, economic and security elites. In order to identify and exploit vulnerabilities in target countries, Russia mainly used traditional methods of diplomacy and coercion – the establishment of loyal political and cultural organisations, obtaining economic influence, the development of media companies, encouraging separatist movements and anti-government feelings – in order to put pressure on the target state. Briefly, the preparatory phase of hybrid war crisis in Ukraine can be characterised by citing Stanislav Levchenko, a former KGB officer who defected to the US in 1979: *"Identify your weaknesses and there you will find that KGB is involved"*[26]. In conclusion, we can say that the preparatory phase of hybrid warfare war is built based on the traditional Soviet *"instruments"* for foreign policy, plus the growing role of non-military means. Through such an approach, it is virtually impossible to determine whether Russia's traditional measures of gaining influence in a certain area means preparing a hybrid war, before triggering the actual attacks. As stated above, the preparatory phase is divided into three stages, as follows:

The preparatory phase was to identify strategic, political, economic, social and infrastructure vulnerabilities of the target state and set the appropriate means for their exploitation. In the case of Ukraine, Russia was favoured in this respect, given their common history, close economic and social ties and close relations between political, economic and security elites.

a) 1st Step – *strategic preparation* comprised a series of activities such as the exploitation of the weaknesses identified in the functioning of the central administration and those recognised at economic and military levels, establishing networks of loyal NGOs and media channels within Ukraine as well as taking positions through diplomatic channels and media to influence the international community;

b) 2nd Step – *political preparation* involved encouraging grievances against the central government, using political, diplomatic, media instruments and special forces as well as an intensification

[25] Andras RACZ, *op. cit.*, p. 57.

[26] A. Weeks, *"A Chilling Expose of KGB and the Reach of its Tentacles; KGB Today: The Hidden Hand by John Barron, Christian Science Monitor*", 03.09.1983, available at http://www.csmonitor.com/1983/1103/110307.html, retrieved on 26.09.2018

ROMANIAN MILITARY THINKING

of separatist movements and fuelling ethnic, religious and social tensions. Also, in this stage information operations were triggered against Ukraine; some government officials, politicians and senior military were bribed and then recruited; relations were established with oligarchs and local business people to make them dependent on the attacking state by offering profitable contracts as well as through local organised crime groups;

c) 3rd Step – *operational preparation* involved political lobbying in coordination with disinformation, the *"activation"* of organised crime groups and recruited officials and soldiers, as well as mobilising Russian armed forces under the pretext of military exercises.

Within the attack phase, the vulnerabilities identified and exploited in the preparatory phase became surprisingly apparent at the outburst of the hybrid offensive on all levels of expression – political, diplomatic, economic, military and information. From this moment on, this hybrid warfare manifested differently than the traditional measures of Soviet foreign and security policy and consisted in triggering open and organised actions, including with armed forces against the target state.

As it can be seen, most of the actions mentioned above are not explicitly illegal or violent, making it difficult to identify and counteract them. Even if the target countries recognise the threats and show concern for countering them, the situation still serves the objectives of Russia, taking into consideration that the pressure felt can generate high responsiveness to the needs and interests of Moscow. Therefore, it can be estimated that the effects of the preparatory phase become visible only in the next phase, when the attack was triggered, practically following the principles set out by Chekinov and Bogdanov and stated above.

2. Within the *attack phase,* the vulnerabilities identified and exploited in the preparatory phase became surprisingly apparent at the outburst of the hybrid offensive on all levels of expression – political, diplomatic, economic, military and information.

From this moment on, this hybrid warfare manifested differently than the traditional measures of Soviet foreign and security policy and consisted in triggering open and organised actions, including with armed forces against the target state. In this context, we can illustrate the similar way in which Russian intervention in Crimea and eastern Ukraine were triggered: military formations without identification elements, with weapons and modern vehicles were rapidly deployed and barricades and checkpoints were set blocking access to Ukrainian police and military units. Although nobody fired any shot, Ukrainian forces were blocked in barracks, unable to leave their premises without using force against Russian militants, aspect that – if it had materialised – would have triggered a conventional intervention of Russian Federation armed forces. Also, occupying political offices

was critical to both interventions, as follows: in Crimea *"the little green people"* occupied the Parliament building and the Supreme Council of Crimea (27/02/2014), thus preventing the functioning of local political system. In Donetsk, the centre of local government residence was one of the first objectives to conquer (April 2014) and the building still is the headquarters of the so-called Donetsk People's Republic (DPO) currently. Ukrainian security forces were unable to protect these symbolic premises, largely due to the lack of precise orders for action, the low morale, the incompetent leaders and inadequate equipment. Meanwhile, civilians who were well-organized, armed and often showing remarkable tactical skills also seized other local government buildings, media offices and infrastructure. Occupying local television and radio headquarters and broadcasting relays had critical relevance because it allowed hackers to cut off Ukrainian channels and replace them with Russian ones. Both *"green men"* and *"civilian attackers"* repeatedly stated that they are locals disgruntled with the central government in Kiev, being constantly supported by Moscow, whose official speech was presented as *"opposition"* or local *"resistance"*. The actions in the field were supported by an extremely intense information campaign, focused on confusing decision-makers, thus generating mistrust, fear and discontent with respect to the central government in Kiev and degrading resilience capacity of Ukrainian armed forces and police, weakening their morale. Moreover, the command and control system of Ukrainian forces was frequently broken, jammed and discredited by sabotage acts, corrupt officials[27] and actions of electronic warfare. The exercise of these pressures by Russia and the hesitant manifestations of Kiev resulted in mass surrender of the Ukrainian armed forces and police culminating with defection events to the Russian side, both in Crimea and in Donbas. While the affiliation of *"civilian attackers"* became apparent quite soon, Moscow vehemently denied its involvement in the conflict, sparking confusion among Western observers, and thus gaining time to create a *fait accompli*. From this point of view, we can say that Russia's denial policy, consistently applied, proved to be a real success in the interventions in Ukraine. In some Western analytical media, assumptions were made according to which in the event

romania2019.eu

The actions in the field were supported by an extremely intense information campaign, focused on confusing decision-makers, thus generating mistrust, fear and discontent with respect to the central government in Kiev and degrading resilience capacity of Ukrainian armed forces and police, weakening their morale.

[27] M. Galeotti, *Hybrid War and Little Green Men: How it Works and How it Doesn't,* E-International Relations, 16 April 2015, http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/, retrieved on 27.09.2018.

ROMANIAN MILITARY THINKING

of triggering an attack on a NATO member state, Moscow would use the same policy of denial, confident that such an approach would prevent the North Atlantic Council from declaring the activation of Article 5 of the Collective Defense Treaty. The result of such a scenario would be the non-involvement of NATO to provide support to the assaulted state or a tardive one, after the attack had already been executed. Although most actions are performed by non-military means, it is important to note that conventional forces also play an essential role in the attack phase. Both in Crimea and in Donbas, Russia amassed massive military forces on the border with Ukraine, thus threatening the possibility of implementing a conventional attack. Thus, Moscow managed to distract the attention of Kiev from the *"real issue"* and block the Ukrainian counterattack options, given that any chance of opening fire on demonstrators would have *"allowed"* Russia to respond through a conventional invasion.

Moscow's aim in both regions was to overthrow local political leadership and, once achieved, it passed to the founding of alternative political centres of power. Andrasz Racz notes that Crimean Council deputies were forced by Russian combatants to vote in support of a referendum on the independence of the province, while in Donbas separatists proclaimed the so-called People's Republic of Donetsk and Lugansk.

Moscow's aim in both regions was to overthrow local political leadership and, once achieved, it passed to the founding of alternative political centres of power. Andrasz Racz[28] notes that Crimean Council deputies were forced by Russian combatants to vote in support of a referendum on the independence of the province, while in Donbas separatists proclaimed the so-called People's Republic of Donetsk and Lugansk. The legitimacy of separatist leaders was constantly fabricated through Russian diplomacy and media, both domestically and internationally. Also, Russian media refers even nowadays to the two self-proclaimed republics as the two state entities created democratically, with legitimate leaders, supported by the majority. This approach is not new in the analytical environment considering similar actions of the Soviet Union in Finland regarding the recognition of Kuusinen as a legitimate leader of Karelia (WWII) or by Babrak Karmal as a leader of Afghanistan after the invasion in 1979. Just like the preparatory phase, the attack phase is divided into three stages, as follows:

a) 4th Step – *the beginning of hostilities* involved organising large-scale anti-government demonstrations and riots in the attacked state and the infiltration of special forces disguised as civilians, to execute sabotage acts, to seize the most relevant administrative offices

[28] Andrasz Racz, *op. cit.*, p. 62.

in the targeted areas (with the help of active or passive police and corrupt officials), in cooperation with local organised crime groups. Also, sabotage acts and provocations were carried out in different areas to divert attention and allocation of resources from the principal threat and a strong campaign of disinformation was launched by the Russian media. Through these actions, Ukraine's options to counter the threats were blocked due to the consolidation of superior conventional forces at its borders by the opponent, intended to illustrate the imminence of an intense conventional attack.

b) 5th Step – *the overthrow of the regional/central political authorities* was achieved by disturbing the functioning of local/regional/central authorities by conquering the administrative offices and the telecommunications infrastructure in target areas, as well as by blocking media channels in Ukraine and establishing monopoly over the information and communications environment. At the same time, the combat capacity of Ukrainian forces was destroyed, through non-military means such as: installing barricades to block the access to/from the military units, bribing commanders and moral degradation. Moreover, the border police units were neutralised, being thus unable to fulfil the required tasks. Meanwhile, diplomatic, media, economic tools and the Russian armed forces exerted strong pressure on Ukraine. Russian media channels developed campaigns to mislead the international community and denigrate the target state.

Establishing alternative political power was achieved by decreeing the legitimacy of a new alternative political organisation, citing real or fabricated traditions of separatism from the Ukrainian authorities. Later, political bodies were replaced by some newly created ones. Furthermore, Russian media supported the legitimacy of new political bodies, at the same time influencing the degree of dissatisfaction of the local population with respect to central government through information manipulations.

c) 6th Step – *establishing alternative political power* was achieved by decreeing the legitimacy of a new alternative political organisation, citing real or fabricated traditions of separatism from the Ukrainian authorities. Later, political bodies were replaced by some newly created ones. Furthermore, Russian media supported the legitimacy of new political bodies, at the same time influencing the degree of dissatisfaction of the local population with respect to central government through information manipulations. Thus, the options of countering Ukraine were still blocked by the imminence of a major conventional attack, carried out by conventional forces deployed near the borders.

Considering the examples in Crimea and Donbas, we can say , at the end of the attack phase, the resistance potential of Ukraine was neutralised and the capacity for self-governance and capabilities of communications and command and control were severely damaged,

resulting in the loss of control over parts of the territory. It is believed that Moscow's success would not have had such magnitude without the identification and effective exploitation of Ukrainian vulnerabilities presented during the preparatory phase.

3. *Stabilisation phase*. In order to consolidate the results obtained during the attack, the aggressor state will continue to take additional measures in order to strengthen and legitimise its domination. Regarding the settlement of the conflict in Ukraine, the Donbas scenario turned out to be very different from that in the Crimea, although initially both of them followed the same pattern (referendums were held for independence in both regions, both won by Russian separatists). In Crimea, according to *"official"* results, 87% of the peninsula population participated in the vote and 97% of them were in favour of the independence. One month later, in statistics[29] of Human Rights Council in Russia, accidentally published on the internet, it was reported that only 30% of the eligible population participated in the polls and only 15% of them were in favour of the split. The pressure exercised by the Russian troops still stationed in the peninsula and the separatist forces resulted in the annexation of Crimea by Moscow, after less than one day of its *"independence"*.

Regarding the settlement of the conflict in Ukraine, the Donbas scenario turned out to be very different from that in the Crimea, although initially both of them followed the same pattern (referendums were held for independence in both regions, both won by Russian separatists). In Crimea, according to "official" results, 87% of the peninsula population participated in the vote and 97% of them were in favour of the independence.

In eastern Ukraine, the separatist movement did not have the same success due to low support from the local population and the lack of Russian military units in the region. Igor Strelkov, Colonel of Russia's domestic intelligence service and Defence Minister of the self-proclaimed People's Republic of Donetsk, for a short time, publicly stated that the scenario in Crimea would have been possible in Donbas too, if Russian troops were stationed on the territory of the region[30]. Although separatist forces managed to overthrow Ukrainian regional authorities, subsequently they could not control the territory gained, because of Russia's conventional non-involvement. Thus, rather than establishing a functional alternative power, a state of conflict was created, characterised by political, social and security instability.

[29] P.R. Gregory, *"Putin's Human Rights Council Accidentally Posts Real Crimean Election Results"*, Forbes, 5 May 2014, available at http://www.forbes.com/sites/paulroderickgregory/2014/05/05/putins-human-rights-council-accidentally-postsreal-crimean-election-results-only-15-voted-for-anexation/, retrieved on 29.09.2018.

[30] Euro Maidan PR, *"Russian FSB Colonel Strelkov Admits Crimean MPS Were Forced to Vote for Referendum"*, www.youtube.com, 27 January 2015, available at https://www.youtube.com/watch?v=mcCqrzctxH4, retrieved on 29.09.2018.

Meanwhile, Kiev realised that Russian military forces deployed near the borders would not attack because of the high political stake and decided to launch a joint operation against Russian separatists (called *"The Anti-Terrorist Operation"*, initiated on 04.15.2014). The offensive had a hesitant start, largely due to low morale, lack of unity of command and outdated equipment. This was observed on 16.04.2015, when a Ukrainian column of armoured vehicles was stopped and captured by civilians and separatists without firing a single shot. In May 2015, referendums were held in Donetsk and Luhansk regions in a totally chaotic manner. While, in Luhansk, the population was asked in regard to the declaration of independence, in Donetsk voters were asked to choose between independence and enlarged autonomy. The official results were like those in Crimea, in the sense that most of the population was in favour of independence of Ukraine. The media channel *"Voice of Russia"*, controlled by the Kremlin, referred to the separatist territories as *"republics"* and Roman Lyagin was presented as *"head of the election commission"*, although he was not democratically elected in this position, but named so by pro-Russian separatists. The same media channel did not mention that the international environment condemned the referendums, dismissing them as illegal, given that they were not organised according to Ukrainian laws. However, the purpose of involving Russia in Donbas was different from the Crimea, in that it failed to annex the separatist territories. The exact reasons for which Moscow was not involved in the same aggressive manner in Donbas are still unknown, but it is estimated that a decisive role was played by the potential political and economic repercussions in the West; the greater territory of Donbas as compared to the Crimean territory and the resistance of Ukrainian armed forces.

In May 2015, referendums were held in Donetsk and Luhansk regions in a totally chaotic manner. While, in Luhansk, the population was asked in regard to the declaration of independence, in Donetsk voters were asked to choose between independence and enlarged autonomy. The official results were like those in Crimea, in the sense that most of the population was in favour of independence of Ukraine.

From the perspective of hybrid warfare, I consider that the war in eastern Ukraine has reached the stage of *"frozen conflict"* and is open to the following two scenarios: one option would be the annexation of the territory by Russia, replicating the Crimea case, while the second option is to accept Donbas as part of Ukrainian territory without recognising the authority of Kiev in the region. By making an inductive analysis of the example in Ukraine, I consider that regardless the manner of conflict settlement, the political outcomes and the goals of the hybrid warfare waged by the attacking state will be reached: the strategic freedom of movement of the attacked state (including

here the freedom to choose their foreign policy orientation) will be severely limited due to the loss of territory and therefore to the reduced number of population, resources and the damaged credibility of central authorities. The Ukrainian case demonstrated how hybrid warfare could interfere with the functionality of a state, without attracting it in a conventional war. The stabilisation phase is described in three stages:

a) 7th Step – *political stabilisation* was achieved by organising a referendum regarding the independence/splitting of the region concerned, with strong diplomatic and media support from the attacking state. Thus, the *"new state"* calls for support from the attacking state.

Separating the territory captured from the target state comprises two sub-stages: the attacking state annexes the captured territory (Crimea) and the attacking state ensures military presence (openly or covert) and conducts military actions against the target state under the pretext of supporting the new state, degrading it politically, economically and militarily (Donbas). An alternative could be an open invasion under the pretext of "peacekeeping missions" or "crisis management".

b) 8th Step – *separating the territory* captured from the target state which comprises two sub-stages: the attacking state annexes the captured territory (Crimea) and the attacking state ensures military presence (openly or covert) and conducts military actions against the target state under the pretext of supporting the new state, degrading it politically, economically and militarily (Donbas). An alternative could be an open invasion under the pretext of *"peacekeeping missions"* or *"crisis management"*.

c) 9th Step – *the strategic freedom of movement* of the attacked state was limited on the long-term by the loss of territory which attracted severe economic difficulties, political instability and a serious humanitarian crisis. Due to the loss of control over the territory, Ukraine cannot join any international military and political alliance in which territorial integrity is required.

However, given the recent developments in the security situation in eastern Ukraine, I consider that a lesson learned, already established, is confirmed in this case as well: irregular forces cannot deal with an attack planned and executed by conventional forces. In order to protect its strategic interests and separatist movement in Donbas, Moscow was also involved in a conventional manner (although without admitting this), thus turning the war in eastern Ukraine into a conventional conflict, limited in scale, which became *"frozen"* after the current testing between Moscow and Kiev, mediated by the international environment.

Hybrid warfare is built on exploiting the vulnerabilities of a state, on the persecution of its negative aspects at political, economic

and social levels. If an opponent cannot identify enough vulnerabilities, it is estimated that it cannot trigger a substantial attack on the opponent; thus the hybrid war will not reach the second phase – the attack. It is concluded therefore that the best defence against hybrid warfare is a stable and viable government. However, the viability of governance must be understood in a broad sense, which, in addition to the smooth democratic functioning, also includes the observance of human rights, the freedom of the press, the respect and integration of ethnic and religious minorities, the elimination of corruption generating insurgency, aspects meant to ensure the legitimacy of governing, contributing significantly to the stability of the state.

Hybrid warfare is built on exploiting the vulnerabilities of a state, on the persecution of its negative aspects at political, economic and social levels. If an opponent cannot identify enough vulnerabilities, it is estimated that it cannot trigger a substantial attack on the opponent; thus the hybrid war will not reach the second phase – the attack. It is concluded therefore that the best defence against hybrid warfare is a stable and viable government.

Elements of operational art of the conflict in Ukraine

The relative success of Russia in taking military control over the south and east of Ukraine is explained mainly through the superiority of this new *"paradigm of conflict"*. In addition, the determining factor, common to both areas of military operations in Ukraine, Crimea and Donbas, was the presence of a controlling pro-Russian population of Orthodox religion, willing to cooperate and support the Russian military forces and the paramilitary pro-Russian forces in their actions to gain control over Ukrainian territory. Another factor favouring the accomplishment of the Russian forces' mission was the one represented by the refusal of an important part of the Ukrainian security "establishment" to participate in operations against military Russian aggression in Ukraine, whether for ideological reasons, or by considering such an endeavour as purely suicidal.

By making a realistic assessment of the regional security environment and the characteristics of the two areas of operations, the Russians were able to easily identify the vulnerabilities of the Ukrainian opponents and employ a wide range of attacks, from the information-symbolic subversive ones, designed to alter the political decision-making processes of Ukrainians, to the mobilisation, at tactical level, of paramilitary forces on Ukrainian territory to execute actions for occupying administrative centres, police stations, airports, military depots, destruction of transport infrastructure which would have favoured the Ukrainian attacks determined to counter the actions of pro-Russian insurgent forces.

Simultaneously, at the operational level, the Russians deployed on the border with Ukraine forces that were on battle alert and periodically executed various complex military exercises, involving all the services, meant to deter a vigorous Ukrainian military intervention which might restore sovereignty over the territories retrieved under control of pro-Russian forces. In support of paramilitary forces, in areas close to the Ukrainian border, the Russians created logistics and training bases for pro-Russian insurgents that were later organised into groups of battalion level, equipped with tactical combat arms and led by Russian officers.

At the operational level, the Russians deployed on the border with Ukraine forces that were on battle alert and periodically executed various complex military exercises, involving all the services, meant to deter a vigorous Ukrainian military intervention which might restore sovereignty over the territories retrieved under control of pro-Russian forces.

At the strategic level, Russian armed forces were alerted; mobile tactical nuclear missile sub-units were deployed towards the western borders of the Russian Federation and they manoeuvred units of intercontinental missiles, performed aggressive patrols with strategic aviation in the areas concerned, all of these in order to discourage any possible form of foreign military involvement in the crisis in Ukraine.

In carrying out combat actions in Ukraine, the Russian armed forces and the pro-Russian paramilitary forces efficiently used some weapons systems that ensured freedom of movement in the tactical field, as follows:

a. *Air defence systems.* These systems used in a network and integrated with other categories of forces, secured through number and density of layout, Russian superiority and air supremacy in Donbass region. Especially self-propelled and portable air defence systems blocked nearly all the Ukrainian military aircraft in its own airspace. Also, Ukrainian combat helicopters had to fly at distances of three to five meters from the ground or at the outskirts of the woods to avoid self-propelled missile defence systems but becoming vulnerable to ambushes made by the teams of insurgents armed with portable rocket launchers.

b. *Unmanned aerial systems.* In Ukraine, there was one of the first air confrontations in which parties made extensive use of unmanned aerial systems (UAS). Russia used these systems for intelligence, surveillance and reconnaissance, target acquisition and real-time engagement in support of massed artillery barrages; a novelty in the use of UAS was to use them as mini-firebombs remote-controlled and directed towards ammunition depots, hydrocarbons and other easily inflammable materials. A psychological effect of using UAS

was noticed among Ukrainian combatants who realised the permanent risk of having own devices located by Russian UAS, which inhibited their movement and manoeuvre, especially during the day.

c. *Electronic warfare systems*. Electronic warfare systems were used for:

- blocking the opponent's communications – in Donbas, there were areas where no electromagnetic communication system (radio, mobile phone, TV) worked;
- disrupting the unmanned aerial systems (UAS) by jamming both UAS control system and GPS signal;
- disrupting Ukrainian artillery and mortars bombs by exploding electronic warheads ammunition on trajectory;
- disrupting command and control nodes by identifying electromagnetic emissions (radio, Wi-Fi, GSM, locator of own troops) and their subsequent utilisation through UAS and destroyed by massed artillery shootings.

d. *Massed fire.* The ability to acquire information dominance over the airspace through permanent surveillance combined with the ability to perform high-precision shooting with multiple launchers of reactive projectiles ensured enhanced lethality. The features of the ammunition used – thermo-baric munitions, sub-munitions – used in preplanned massed shooting produce catastrophic effects to the vital force and technology of the opponent.

The ability to acquire information dominance over the airspace through permanent surveillance combined with the ability to perform high-precision shooting with multiple launchers of reactive projectiles ensured enhanced lethality. The features of the ammunition used – thermo-baric munitions, sub-munitions – used in preplanned massed shooting produce catastrophic effects to the vital force and technology of the opponent.

e. *Heavy armoured vehicles.* Tanks remain decisive on the battlefield if they have multilayer armour and are equipped with active protection systems against anti-tank missiles guided or launched by the enemy infantry troops. Also, the use of tanks fitted with radars for laser tele-metrics identification by the enemy and the trajectories of anti-tank missiles launched by them, as well as modern computerised systems of control/fire control, with advanced optical systems able to accurately identify targets in all weather conditions and at night ensure tank manoeuvrability and the lethality required for dominating the land battle space.

f. *Opportunities to counter Russian conventional actions*. From military perspective, kinetic Russian actions in Ukraine could be countered through tactical and operational decisions relatively easy to implement:

- in order to counter Russian electronic warfare measures it is necessary for the opponent to hold and use analogue

capabilities, restrict to a minimum the number of electromagnetic transmitters (example: mobile phones), to direct the antennas as far as possible from control centres and equip tactical level combat forces with capabilities of combating the Russian offensive electronic measures;

- in case the opponent uses unmanned aerial systems (UAS), it is necessary that own forces are involved in concealing, harbouring and misleading the enemy about own layout, formation and intentions, the location of key systems, permanently assuming the hypothesis that it evolves under constant aerial surveillance. Equally, at the tactical level (ex. company), forces must be equipped with target acquisition and firing systems against opposing UAS;
- the increased dispersion of enemy combat forces in the tactical field calls for being equipped with artillery pieces with intelligent ammunition and augmented striking range, assisted in locating, identifying, acquiring and hitting enemy targets by own UAS and protected by capabilities able to counter enemy artillery. The combined use of artillery and these capabilities of counteracting enemy shooting requires the opponent to *"uncover"* to modify the shooting position or to perform other types of manoeuvre, thus becoming vulnerable to own shooting;
- Russian tanks remain powerful in the tactical field, being equipped with additional reactive armour. To be annihilated, own tanks must be at least as protected and the infantry troops have to be equipped with anti-tank guided portable missiles using ammunition able to annihilate the protection offered by this type of armour;
- Russians used combat tactical groups of battalion level in battles in Ukraine, consisting of a tank company, three mobile infantry companies, an anti-tank company, two or three companies of self-propelled guns and multiple-launch rocket systems and two air defence companies. These organic sub-units provide lethality, manoeuvrability and protection necessary to operating in the tactical field in a decentralised and dispersed manner. In order to deal with these capabilities, it is necessary to return to the structure of armoured

In case the opponent uses unmanned aerial systems (UAS), it is necessary that own forces are involved in concealing, harbouring and misleading the enemy about own layout, formation and intentions, the location of key systems, permanently assuming the hypothesis that it evolves under constant aerial surveillance. Equally, at the tactical level (ex. company), forces must be equipped with target acquisition and firing systems against opposing UAS.

"regiment" with full capacity of forces and fire manoeuvre, air and logistical support.

The Russian example of coordination and centralization of *"total conflict"* management, the most relevant observable confrontation in eastern Ukraine, demonstrates that Russian operative art evolves constantly synchronising with the historic developments in the field of information technology and adapting its Soviet experience to contemporaneity. Russian political elite is able to enforce the principle of unity of design, command and control at all levels of implementation of security and defence strategy of the Russian Federation, which ensures efficiency in reactions, often surpassing the Western reaction in terms of initiative and creativity.

Arguments proving the efficiency of hybrid warfare in Ukraine

Despite the partial failure in Donbas, the hybrid war waged by Russia in Ukraine is overall considered as a success. In order to understand the reasons that facilitated the efficiency of Russian actions, one should consider the factors that favoured Moscow's conduct in time and space, some being general in nature, while others were characteristic to the Ukrainian environment, as follows:

a. *The element of surprise.* The first and probably the most important factor of general nature that led to the efficiency of hybrid warfare in Ukraine was the element of surprise. Although neither Moscow's strategic position nor the inherent weakness of the Ukrainian state were new, the rapid implementation by the Russian Federation of the entire spectrum of hybrid warfare (the three phases presented above) succeeded in taking by surprise both authorities in Kiev and the West. This form of war had never been used in this configuration and, as such, the defensive means to combat it were undeveloped. In addition, Russia misled both Kiev and the West through actions of concealment and information intoxication. According to an article published in *"Voenno-promishlenniy Kurier"* (September 2014) by Russian General Anatoly Zaitsev, one of the key elements of success was the absence of radio traffic within the Russian forces before the start of operations, combined with extensive disinformation operations[31]. This favoured

The first and probably the most important factor of general nature that led to the efficiency of hybrid warfare in Ukraine was the element of surprise. Although neither Moscow's strategic position nor the inherent weakness of the Ukrainian state were new, the rapid implementation by the Russian Federation of the entire spectrum of hybrid warfare (the three phases presented above) succeeded in taking by surprise both authorities in Kiev and the West.

[31] A. Zaitsev, *Voenno-promishlenniy Kurier*, No. 32 (550), 3 September 2014, available at http// www.vpknews.ru/articles/21649, retrieved on 23.11.2018.

ROMANIAN MILITARY THINKING

the surprise element that, effectively used in combination with information intoxication, brought Russia a decisive advantage against Ukraine – and probably would have had the same effect against other opponents, especially in areas with a significant Russian minority. Another factor, this time particular to Ukraine was the effective use of Russian military base in Sevastopol and the Black Sea fleet vessels that were used for rapid deployment of troops participating in the operation. In the same article, General Zaitsev mentioned that *"polite green people"* appeared right on time and wherever needed to counteract the Ukrainian forces. Thus, we can say that the essential means of misleading Kiev and the West was the use of highly efficient and well-coordinated information war. Moscow allocated time and resources to build this capability[32] and was quite clever not to disclose its full potential before the decisive moment of the attack. So, the remarkable power of information warfare - both in Ukraine and in the West – was another surprise element. Kiev was not ready to counter such attacks and as a result was totally surprised by the speed of their deployment, as would otherwise have been many other states, being forced to adopt a defensive and almost permanently reactive position.

Ukraine faced the delicate situation of having no negotiating partner as the Russian Federation refused to talk, vehemently stating its non-involvement in the conflict. Meanwhile, Moscow followed the old familiar pattern from the conflicts of the '90s, inviting Kiev to negotiate directly with the separatists. Obviously Ukrainian leadership did not accept this alternative because it would have meant "de facto" recognition of separatists as legitimate partners.

b. *Denying the involvement in the conflict.* Another factor of general nature was the permanent denial Moscow regarding its involvement in the conflict, aspect which created confusion within the central office in Kiev and generated no reaction from the West, allowing Russia to gain time. Also, attackers enjoyed the benefits of *"the lack of identity"*, given that their membership was not visible to any nation state and there was no formalized institutional subordination. Thus, Ukraine faced the delicate situation of having no negotiating partner as the Russian Federation refused to talk, vehemently stating its non-involvement in the conflict. Meanwhile, Moscow followed the old familiar pattern from the conflicts of the '90s, inviting Kiev to negotiate directly with the separatists. Obviously Ukrainian leadership did not accept this alternative because it would have meant *"de facto"* recognition of separatists as legitimate partners. Moreover, denying the involvement in the conflict would have allowed Russia, at least theoretically, to be able to stop hybrid attacks at any time in case in which the developments in the field would not have been consistent with the operational plans. In other words, denying involvement allows the stopping of a hybrid war at any time, even if the phase of the attack was already initiated, as long as no political acts are performed that might compromise the irreversibility of such a decision. By simply removing the forces without identifying elements and giving orders to undercover agents to calm down violent demonstrations and stop the actions of sabotage, Moscow would have been able to leave Crimea and Donbas quietly and without repercussions. It was therefore an alternative within Kremlin reach, which eventually had no reason to use.

romania2019.eu

c. *The failure to distinguish between the civilian population and the attackers.* Another contributor to the efficiency of hybrid offensive was shown by the fact that many of the attackers were equipped in civilian clothes, making it impossible to distinguish between them and the locals. Thus, the potential of Ukrainian forces to use force against separatists was limited for several key reasons. First, Kiev could not afford the risk of killing Russian locals, as this would have attracted a large-scale military intervention from Russian Federation under the pretext of defending the Russian-speaking population. Even if this happened in Ukraine, I consider that this factor is not specific just to Ukraine, because such a threat from Russia may occur in other countries too, where the Russian minority is strongly represented. Furthermore, other factors that favoured the attackers' impossibility of spotting and tracing Russian aggressors have a highly specific Ukrainian character. Ukraine lacked organised and well equipped police forces which might have been able to identify and counter these threats. It should be recalled that the famous special forces of the interior ministry, known as *"Fist of Steel"* or police unit *"Berkut"* were only loyal to the dismissed president Viktor Yanukovich, many members manifesting their adhesion to Russians separatists after they fled. After the regime change in Kiev, the *"Berkut"* unit was dismantled (February 2014) as a result of the multiple accusations of murder committed by its members during the Euro Maidan protests. However, the disbanded unit was not replaced by any other similar capability, Ukraine being thus deprived of special units for controlling the crowds during the violent demonstrations that followed. Consequently, regular Ukrainian police forces proved unable to manage the violent protests orchestrated by the Russian Federation, either because

Regular Ukrainian police forces proved unable to manage the violent protests orchestrated by the Russian Federation, either because of a lack of capacity of mobilisation and rigorous command or due to the low morale that generated fear of commitment and accountability. Simultaneously, Russian propaganda proved effective in discrediting the legitimacy of the new government in Kiev, leading to uncertainty among police forces and uncertainty regarding the legal character of the orders to be carried out.

[32] K. Gilles, *Russia's Hybrid Warfare: A Success in Propaganda*, Working Paper, 2015/1.

ROMANIAN MILITARY THINKING

of a lack of capacity of mobilisation and rigorous command or due to the low morale that generated fear of commitment and accountability. Simultaneously, Russian propaganda proved effective in discrediting the legitimacy of the new government in Kiev, leading to uncertainty among police forces and uncertainty regarding the legal character of the orders to be carried out. Consequently, cases were reported of police chiefs being replaced from the management of units or defecting to separatist movements. It was also found that many members of the regular police forces did not accept the risk of fighting to defend the offices of local government institutions for fear of potential repercussions on their careers, preferring to remain idle at the actions of the demonstration participants. Thus, it is considered that the absolute factor, particular to Ukraine, which explains the success of hybrid Russian offensive was the severe and prolonged impairment of the government in Kiev[33].

The hybrid warfare concept was born and has recently developed within the framework of American military thinking, generated by the evermore increasing complexity of the confrontation environment and the necessity of adapting the political-military strategies of this phenomenon.

Conclusions

The physiognomy of military conflicts during the post-Cold War period was characterised by substantial transformations resulting mainly in the evolution from symmetric to asymmetric and from linear to non-linear. At the same time, given the expansion of globalisation and technical-scientific progress, the unconventional feature became prevalent over the whole range of conflicts. This, in turn, generated a dilatation of the confrontation space and a diversification of the types of threats to the global security environment[34].

With respect to the hybrid warfare concept, this was born and has recently developed within the framework of American military thinking, generated by the evermore increasing complexity of the confrontation environment and the necessity of adapting the political-military strategies of this phenomenon.

The decentralised planning and execution of actions in a hybrid conflict/war allow a very high degree of adaptability which the classical structures, with their complicated decision making chain of actions cannot afford, but, at the same time, they result in the impossibility of detecting the enemy's belonging, their chain of command and connections, which increases the countering of a hybrid threat.

[33] Andrasz Racz, *op. cit.*, p. 70.

[34] Col. Liviu Ioniță, *op. cit.*, p. 32.

romania2019.eu

Moreover, the development of hybrid conflicts does not represent an end of traditional or conventional warfare, but a factor which complicates 21st century defence planning. These implications may be highly significant in nature which leads to the necessity of hybrid conflicts being settled through innovative thinking[35].

The unanimously embraced opinion is that hybrid warfare consists in the coordinated use of military and non-military means in order to obtain synergic effects in the physical and psychological dimensions of the conflict. Just as we have mentioned in the lines above, there is a tendency of regarding *"hybrid warfare"* as the *"new generation warfare"*, notion emerging after Gulf War (1991), the Arab Spring (2011) and Russian Federation's recent interventions in Ukraine (2014). Analysing the evolution of the typology of conflicts as well as the peculiar character of the action environment in Ukraine for Russian armed forces, we consider that the analytical concept of *"hybrid warfare"* is going to have an ephemeral character and should not be regarded as the *"successful recipe"* of future conflicts. It is risky to believe that any *"new"* approach to warfare, including here *"hybrid warfare"* too, may lead to repeated victories; this perspective reflects what analyst Hec Strachan[36] calls an "a-strategic" approach of warfare, though which operational and doctrinal capabilities are over-estimated within strategies. In other words, the assumption that a certain kind of warfare or doctrinal approach is going to result in victory, no matter the circumstances, ignores the fact that the success of a strategy always relies on the context. Thus, winning formulas such as *"strategic bombing"*, *"asymmetric warfare"*, *"network-centric warfare"*, *"full-spectrum warfare"* or *"hybrid warfare"* must not be taken as strategies, but rather as means to a desired end-state or merely the "operational approach" that contributes to the fulfilment of the strategic effect. These concepts may be successful only if they perfectly adjust to the circumstances of each particular conflict and, in most cases, they cannot prevent the unavoidable military confrontations, chaos or even humanitarian disasters.

It is true that such situations were avoided in Crimea, but here we need to take into account the circumstances of the environment

[35] Frank G. Hoffman, *op. cit.*, p.5.

[36] Hew Strachan, *The Direction of War: Contemporary Strategy in Comparative Perspective, Cambridge, Cambridge University Press*, 2013, p. 13.

ROMANIAN MILITARY THINKING

that favoured the „hybrid" character of Russian intervention – the existence of a significant pro-Russian community, the presence of Russian military units and corresponding personnel that favoured the infiltration of special operations forces in Russia, the Ukrainian corrupt and inefficient political leadership, the almost complete absence of Ukrainian forces' armed resistance, the lack of reaction of the international community, taken aback by the rapidity of action of Russian forces. Thus, we consider that the Russian strategy worked in Crimea as the variety of military and non-military means used were in complete accordance with the favourable context characterised by the factors mentioned above and not because the Russian Federation developed a new and complex approach of winning wars.

The Russian strategy worked in Crimea as the variety of military and non-military means used were in complete accordance with the favourable context characterised by the factors mentioned above and not because the Russian Federation developed a new and complex approach of winning wars.

Yet, there was a completely different situation in the Eastern Ukraine where Russian intervention did not benefit from the anticipated support of Russian-prone population and had to face a better organized resistance of Ukrainian army, aspects that led to a prolongation of the conflict and, inevitably, to changing its nature into a preponderantly conventional one, with high material and human losses that generated a significant humanitarian crisis in the region.

BIBLIOGRAPHY

1. ***, Euro Maidan PR, "*Russian FSB Colonel Strelkov Admits Crimean MPS Were Forced to Vote for Referendum*", www.youtube.com, 27 January 2015.
2. ***, NATO, *Wales Summit Declaration*, 5 September 2014.
3. J. Berzins, *Russia's New Generation Warfare in Ukraine: Implication for Latvian Defence Forces*, National Defence Academy of Latvia, Center for Security and Strategic Research, 2014.
4. S. Chekino, S. Bogdanov, *The Nature and Content of a New-Generation War*, in *Military Thought*, October-December 2013.
5. M. Galeotti, *The „Gerasimov Doctrine" and Russian Non-Linear War*, 6 July 2014, http://cs.brown.edu/people/jsavage/VotingProject/2017_03_09 _MoscowsShadow_ GerasimovDoctrineAndRussianNon-LinearWar.pdf.
6. M. Galeotti, *Hybrid War and Little Green Men: How it Works and How it Doesn't*, E-International Relations, 16 April 2015.
7. Michael S. Gerson, *Conventional Deterrence in the Second Nuclear Age*, Army Strategic Studies Institute, 2009.
8. K. Gilles, *Russia's Hybrid Warfare: A Success in Propaganda*, Working Paper, 2015/1.
9. R. Glenn, *Thoughts of Hybrid Conflict*, in *Small Wars Journal*, 2009.
10. P.R. Gregory, *Putin's Human Rights Council Accidentally Posts Real Crimean Election Results*, in *Forbes*, 5 May 2014.
11. F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, Virginia, December 2007.
12. Petri Huovinen, *Hybrid Warfare – Just a Twist of Compund Warfare*, National Defence University, 2011.
13. Colonel Liviu Ioniță, *Fizionomia conflictelor contemporane. Ascensiunea abordărilor neliniare*, doctoral thesis, „Carol I" National Defence University, Bucharest, 2015.
14. Douglas Mastriano, *Defeating Putin's Strategy of Ambiguity*.
15. J.J. McCuen, *Hybrid Wars*, in *Military Review*, March-April 2008.
16. Andras Racz, *Russia's Hybrid War in Ukraine*, The Finnish Institute of International Affairs, https://www.fiia.fi/en/publication/russiashybrid-war-in-ukraine.
17. Hew Strachan, *The Direction of War: Contemporary Strategy in Comparative Perspective*, Cambridge, Cambridge University Press, 2013.
18. A. Weeks, *A Chilling Expose of KGB and the Reach of its Tentacles; KGB Today: The Hidden Hand*, by John Barron, in *Christian Science Monitor*, 3 September 1983.
19. M. Williamson-P. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, Cambridge, 2012.
20. A. Zaitsev, *Voenno-promishlenniy Kurier*, nr. 32 (550), 3 September 2014.

romania2019.eu

COMBATING HYBRID THREATS AT THE EUROPEAN UNION LEVEL

Captain BEng Viorica Ionela TRINCU

PhD candidate, "Carol I" National Defence University

Nowadays, the greatest challenges to the nations, their institutions, population and private companies are those that are geared towards exploiting their vulnerabilities. At both NATO and EU level, state and non-state actors generate a series of visible and undercover activities that can be referred to as hybrid threats. This article analyses the ongoing process and methods to counter hybrid threats at European level. Since Russia's aggression against Ukraine in 2014, we have learned that there is no cutting edge system or a one-size-fits-all solution we can just buy to reduce these threats.

Combating hybrid threats must be a continuous and dynamic activity that can predict the signs indicating the preparation and conduct of hostile hybrid actions in order to timely employ proper means and tools.

Keywords: hybrid threats, resilience, strategic communication, NATO-EU cooperation.

1. Introduction

The strategic objectives of the new political-military context, which will probably change the current political-military arrangement in Europe in depth, are embodied in a new theory of war, mainly based on the new perception of the notion of *security*. Thus, we note that the relationship between the notions of *security* and *defence* is increasingly determined by the perception of the citizen of how existential normality is affected and of the awareness of the use of protective means and defence actions.

The relationship between the notions of security and defence is increasingly determined by the perception of the citizen of how existential normality is affected and of the awareness of the use of protective means and defence actions.

Many of the current challenges to peace, security and prosperity in the Eastern and Southern neighbourhood of the European Union (EU) further emphasise the need for the Union to increase and adapt its capacities as a provider of security, with a strong emphasis on the close link between external and internal security. Internal vulnerabilities and failures of the states, overlapping with external influences, are the main causes of threats and conflicts[1]. The complexity of the international security environment forces political leaders to bear in mind that security can no longer be analysed in terms of political choice, capacities and intentions of a single state or of a single non-standard entity, whereas vulnerabilities, risks and security threats have achieved systemic connotation. In this respect, the president of the European Commission, Jean-Claude Juncker, stressed that we must "*strive for Europe to be stronger in security and defence*" and that European and national instruments must be correlated in a more effective way than in the past[2].

The European security environment has radically changed mainly because of two factors that dominate the security agenda. The first

[1] Mihail Orzeață, *The War Humanity Has always Waged against Itself,* Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovak Republic, 2012, p. 208.

[2] *Document de reflecție privind viitorul apărării europene*, Comisia Europeană, Bruxelles, 2017, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2017:0315:FIN:RO:PDF, retrieved in December 2018.

is the aggression of Russia against Ukraine, including the annexation of the Crimea Peninsula, which has subjected the fundamental principles of international law to great challenges. In this context, the widespread and very well-coordinated use of sophisticated hybrid warfare tactics has compromised Ukraine's territorial integrity and has also influenced the security situation in the region. In addition, by ambiguity and masked threats, Russia has attempted to dismember the international community, including by portraying the EU as an instigator in this conflict.

The second is represented by the actions undertaken by ISIL/Da'esh that have fuelled regional instability, while at the same time manifesting the danger that other terrorist organisations, such as BOKO HARAM and Al-Shabaab, will follow his example. The aggressive ideology of Da'esh attracted thousands of young Europeans who, renouncing European values, joined the ideas of the Holy War as "*foreign fighters*". Their return to Europe could have significant negative consequences.

Hybrid warfare involves coordinated, direct and open or covert use of a wide range of military and civil, conventional and non-conventional instruments/ tactics in an aggression against another state, without the involvement of the use of its territory. These tools can be used individually or concerted.

2. Conceptual limitations

Hybrid warfare involves coordinated, direct and open or covert use of a wide range of military and civil, conventional and non-conventional instruments/tactics in an aggression against another state, without the involvement of the use of its territory. These tools can be used individually or concerted. By using hybrid tactics, the attacker wants to undermine and destabilise an opponent by applying coercive and subversive methods. These include various forms of sabotage, interruption of communications and other services, such as energy supply and resources of all kinds. Massive disinformation campaigns dedicated to control the written press are an important element of a hybrid action. All this is aimed at obtaining political influence, even dominance over a country, in support of a wider strategy.

A critical aspect of the hybrid war is the generation of a state of ambiguity, both among the population concerned, and on the international community in order to mask what is really happening and to create an obscure situation. Ambiguity can lead to the paralysis of the opponent's ability to react, to affect its potential to mobilise for defence and it is unclear who is behind the attack. Moreover, the state

of ambiguity divides the international community, limiting the range and methods of responding to aggression.

By their destination, hybrid threats will continue to evolve on the basis of the application of technological progress, changes in adverse developments and vulnerabilities and the development of countermeasures. An important factor for the EU is the ability to assess the overall effect and strengthen resilience as a means of countering any possible aggression.

3. Understanding and ascertainment of vulnerabilities

The fundamental feature of a hybrid aggression is that it is intended to exploit the vulnerabilities of the target state. It is very important for EU member states and their partners to become aware of this fact and to reach the most appropriate political and operational decisions to respond appropriately.

The fundamental feature of a hybrid aggression is that it is intended to exploit the vulnerabilities of the target state. It is very important for EU member states and their partners to become aware of this fact and to reach the most appropriate political and operational decisions to respond appropriately.

In the case of Ukraine, critical vulnerabilities were represented by: poor government of the country; widespread corruption; lack of confidence in security and defence structures and their inability to ensure adequate support; the presence of a large group of Russian-speaking inhabitants and their perception that they are marginalised; critical dependence on imports and energy supply from Russia.

For EU member states, the Da'esh threat revealed very sensitive issues such as: vulnerabilities associated with minority integration and social exclusion, on the one hand, and weaknesses inherent in an open society (characterised by freedom of expression), on the other hand, which made the appropriate response to the enlargement of hatred difficult.

All member states have their own vulnerabilities, ranging from economic, energy dependence, critical infrastructure ones, to sensitive issues such as the integration of religious minorities or ethnic groups. While some of the vulnerabilities are specific to each state, others represent challenges for many, or even for all. For example, cyber vulnerabilities are a cause of concern for all member states, even if the level of preparedness and the ability to counter hazardous activities vary from one country to another.

4. EU response

Improvement of the level of ascertainment of the real situation

It is vital that each member state knows its own vulnerabilities, so it is necessary to achieve a high degree of knowledge of the real situation. It is very important to have the ability to identify any changes in the environment of threats, which could represent elements of an extended adverse campaign. Effective knowledge of the real situation is a fundamental requirement and must be supported by the most effective process of exchanging information, good practices and lessons learnt. Within the European institutions, there must be closer cooperation between the relevant structures that are exposed to hybrid threats.

It is vital that each member state knows its own vulnerabilities, so it is necessary to achieve a high degree of knowledge of the real situation. It is very important to have the ability to identify any changes in the environment of threats, which could represent elements of an extended adverse campaign. Effective knowledge of the real situation is a fundamental requirement and must be supported by the most effective process of exchanging information, good practices and lessons learnt.

There are a significant number of indicators, used by a wide range of EU structures, which allow for an effective early warning. In this respect, a virtual information convergence cell transmitted by the member states and the EU institutions, which enables the analysis of various indicators and alert signals triggered by a hybrid action, has been created. This cell centralises all indicators transmitted by EU structures and analyses them in the context of possible hybrid action scenarios, both in the member states and in the partner states.

The authors of hybrid threats can systematically misinform, including through specific campaigns on social media, thus trying to radicalise individuals, destabilise society and control political discourse. The ability to respond to hybrid threats, using the most appropriate ways of strategic communication, is essential. Thus, the EU's communication capacity should be improved, through messages addressed to Russia and the Eastern neighbourhood, in order to respond to possible disinformation campaigns. The EU's strategic Communication to the Eastern neighbourhood should focus its efforts, firstly, on the development of positive and effective messages on EU policies towards the region. Messages should give citizens the possibility of easily understanding that the political and economic reforms promoted by the EU can, over time, have a positive impact on their lives.

Consolidation of resilience

It should be accepted that the drafting and transmission of an appropriate response to countering hybrid threats is a national responsibility. It is the task of each state to minimise its own vulnerabilities. Resilience can be defined as the adaptive ability to cope with changes and disturbances, respecting what experts call elementary differences, in which responses to these disturbances are considered to be particularly important[3].

The drafting and transmission of an appropriate response to countering hybrid threats is a national responsibility. It is the task of each state to minimise its own vulnerabilities. Resilience can be defined as the adaptive ability to cope with changes and disturbances, respecting what experts call elementary differences, in which responses to these disturbances are considered to be particularly important.

The sustained efforts to implement the rule of law, fight against corruption and reform the funding system of political parties are key "*ingredients*" in countering hybrid actions. With regard to the protection of critical infrastructures, the improvement of security requirements will lead to a significant reduction in vulnerabilities.

Both at EU and NATO level, there is currently no strategy to counter hybrid threats, so, given the competences of each of the two organisations, as well as preserving the autonomy of decision, it is an opportune time for cooperation and enhancing complementarity.

Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy, said: "*In recent years, the security environment has changed dramatically. We have seen the rise of hybrid threats on EU's borders. There has been a strong call for the EU to adapt and increase its capacities as a security provider. The relationship between internal and external security needs to be further strengthened. With these new proposals, we want to enhance our capacity to counter threats of hybrid nature. In this effort, we will also step up cooperation and coordination with NATO*"[4].

At the same time, Jorge Domecq, the executive director of the European Defence Agency (EDA), stressed the importance of enhanced cooperation of the Euro-Atlantic relations, which would lead the NATO-EU partnership "*to a new level*". In the current context of the spread of hybrid war-specific threats, stepping up NATO-EU cooperation "*is not*

[3] Reinette Biggs, Maja Schluter, Michael L. Schoon. *Building Resilience. Sustaining Ecosystem Services in Social-Ecological Systems,* Cambridge University Press, Cambridge, UK. 2015, pp. 53-54.

[4] *Securitate: UE consolidează răspunsul la amenințările hibride*, Comisia Europeană, Bruxelles, 2016, http://europa.eu/rapid/press-release_IP-16-1227_ro.htm, retrieved in January 2019.

an option, but an absolute necessity", the EDA executive director said in the presence of the deputy Secretary-General of NATO for Policy and Defence Planning.

Mr. Domecq concluded his speech by stating that *"our collective reply to hybrid is a major opportunity... the comparative advantages of the EU and NATO should be used to the maximum extent. The deterrence effect of NATO and the complementarity of our EU tools and instruments are more than enough reason to enhance our cooperation"*[5].

Resilience could be strengthened by ensuring complementarity in the setting of benchmarks for critical parts of their infrastructure, as well as through close collaboration in the areas of strategic communication and cyber defence. Strengthening resilience to hybrid threats and capacity-building is mainly the responsibility of member states. However, the EU institutions need to take a series of measures to help strengthen national efforts. These include actions carried out in close collaboration with other international actors, notably with NATO[6]*, and such activities could be in depth in the form of support to member states in areas such as the rapid response*[7].

Resilience could be strengthened by ensuring complementarity in the setting of benchmarks for critical parts of their infrastructure, as well as through close collaboration in the areas of strategic communication and cyber defence. Strengthening resilience to hybrid threats and capacity-building is mainly the responsibility of member states.

5. Types of possible actions at the EU level to counteract hybrid threats

- Initiating studies in order to better understand the challenges and establish an inventory of existing instruments and policies or to be developed;
- Including academic personalities, research and excellence centres of the EU and NATO in strategic debates;

[5] Federico Yaniz, *Projecting Stability: Hybrid Warfare and Cooperation with the EU*, 02 February 2018, http://www.atahq.org/2018/02/projecting-stability-hybrid-warfare-cooperation-eu/, retrieved in December 2018.

[6] Countering hybrid threats is one of the seven domains of cooperation with the North Atlantic Treaty Organisation, included in the joint declaration signed in Warsaw in July 2016 by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation.

[7] G7 leaders, reunited in the Charlevoix Summit in June 2018 also agreed upon developing a G7 rapid response mechanism to address threats to democracies: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

- Integrating hybrid issues into the Global Strategy for European Foreign and Security Policy with the aim of identifying objectives, priorities and challenges;
- Rethinking the method of political/military identification and attribution in hybrid threats, as well as interlinking clearly and firmly with hybrid attacks and responses;
- Establishing binding rules for the two cyberspace organisations in order to regulate practices. These rules could serve as guiding principles within various international governmental organisations (UN, OSCE, G20 etc.);
- Developing an European strategy based on current hybrid threats, taking into account all implications – exchange of information, joint exercises, capacity building – and in close coordination with NATO's work;
- Strengthening resilience to hybrid threats of various actors within the EU (member states, institutions) and in particular those relating to transnational networks, irrespective of their nature (economic, energy, transport, communications);
- Developing a strategy and developing early detection and warning capabilities in cyberspace, both at member state and EU level, in which this area is extremely important for cooperation with NATO;
- Reaffirming cohesion and solidarity between member states;
- Enhancing awareness by establishing a European platform. This coordination space could serve as a place where member states can share their experience and lessons learnt;
- Strengthening the strategic communication effort within the EU and its ability to debunk the propaganda of the hybrid war by producing clear, coherent, facts-based information;
- Supporting a free and independent press-backed by strong journalistic ethics, as well as adopting a pro-active communication approach, particularly in the social and media fields;
- Supporting partner states and those in the EU's neighbourhood through exchanges of experience and lessons learnt.

Integrating hybrid issues into the Global Strategy for European Foreign and Security Policy with the aim of identifying objectives, priorities and challenges represents a pertinent action at the EU level to counter hybrid threats.

Developing an European strategy based on current hybrid threats, taking into account all implications – exchange of information, joint exercises, capacity building – and in close coordination with NATO's work, is an essential requirement.

Conclusions

Future conflicts will most likely occur between people and among people, limiting the usefulness of conventional military power applications. This situation will require an integrated, inter/ institutional, non-conventional civilian-military approach to the use of indirect methods and means, with a view to achieving strategic objectives.

In the light of EU documents, actions to help counter hybrid threats, strengthen resilience at EU and national level, and partner resilience require coordinated response actions, the integration of all measures of action taken at the political, diplomatic, information, economic and military levels being the main feature.

In the light of EU documents, actions to help counter hybrid threats, strengthen resilience at EU and national level, and partner resilience require coordinated response actions, the integration of all measures of action taken at the political, diplomatic, information, economic and military levels being the main feature.

Given that the emphasis is on improving awareness, it is recommended the establishment of specialised mechanisms for the exchange of information with member states and the coordination of the EU's ability to provide strategic communications for strengthening resilience in areas such as cyber security, critical infrastructures, protecting the financial system from illicit uses, as well as efforts to fight against violent extremism and radicalisation.

Hybrid threats represent a challenge for both the EU and NATO. The preparation and improvement of an effective response requires dialogue and coordination both at political and operational level between organisations. Closer interaction between the EU and NATO would enable both organisations to prepare and respond effectively to hybrid threats in a complementary way and to support each other on the basis of the inclusion principle while respecting the decision-making autonomy of each organisation and the data protection rules.

BIBLIOGRAPHY

1. ***, *Charlevoix Commitment on Defending Democracy from Foreign Threats*, 2018, https://g7.gc.ca/wp-ontent/uploads/2018/06/DefendingDemocracyFromForeignThreats.pdf.
2. ***, *Document de reflecție privind viitorul apărării europene*, European Commission, Brussels, 2017, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2017:0315:FIN:RO:PDF.

3. *Securitate: UE consolidează răspunsul la amenințările hibride*, European Commission, Brussels, 2016, http://europa.eu/rapid/press-release_IP-16-1227_ro.htm.
4. Reinette Biggs, Maja Schlüter, Michael L. Schoon, *Building Resilience. Sustaining Ecosystem Services in Social-Ecological Systems*, Cambridge University Press, UK, 2015.
5. Mihail Orzeață, *The War Humanity Has always Waged against Itself*, Armed Forces Academy of General Milan Rastislav Štefánik, *Liptovský* Mikuláš, Slovak Republic, 2012.
6. Federico Yaniz, *Projecting Stability: Hybrid Warfare and Cooperation with the EU*, *2018,* http://www.atahq.org/2018/02/projecting-stability-hybrid-warfare-cooperation-eu/.

HYBRID WARFARE - FEATURES AND EFFECTS -

Colonel (r.) Romică CERNAT, PhD

Hybrid warfare seeks victory through the fusion of irregular tactics and the most effective means available in order to attack and achieve objectives in all areas of social life, including politics. Hybrid wars, in fact, combine action capabilities – conventional and asymmetric – cyber, kinetic, media, terrorist and military ones. They employ strategies and tactics, ranging from subversion, cyber-attacks, media manipulation, the presence of combat forces difficult to identify, conducting military exercises to disturbance against constitutional order, crime, agitation and fifth columns. Due to these advantages for the aggressor, it is likely that this form of conflict will persist successfully in the future.

Keywords: instruments of power; vulnerabilities; critical functions; capabilities; escalation; synchronisation.

Preliminary considerations

The international security environment has passed into a new stage, characterised in particular by renewed competition between the three great powers of the world, United States of America, Russia and China. Hybrid wars are a feature of contemporary global politics. The use, by Russia and China, of a new type of military or associated aggressive, paramilitary or intelligence operations – called, among other terms, *hybrid war* or *ambiguous war*, in the case of Russian actions, or so-called small steps tactics or *grey zone war*, among others, in the case of China – represents actions, operations seeking to achieve greater control of neighbouring areas of these two countries. Hybrid conflicts serve to increase ambiguity, complicate decision-making process and slow effective responses coordination.

The new emerging type of hybrid war is a mixture of regular and irregular tactics representing a historical reality on war. The hybrid warfare term emerged during the first decade of the 21st century, when other instruments of power became involved in conflicts and the classic character of past conflicts was blurred.

The new emerging type of *hybrid war* is a mixture of regular and irregular tactics representing a historical reality on war. The *hybrid warfare* term emerged during the first decade of the 21st century, when other instruments of power became involved in conflicts and the classic character of past conflicts was blurred.

World events in recent years, including Chinese actions in December 2013, in the East and South China Seas, and Russia's seizure and annexation of Crimea in March 2014, have led the analysts, since late 2013, to conclude that the international security environment has undergone a change from the familiar post-Cold War era of the last 20 to 25 years, known as the unipolar world, with the United States of America (USA) as the sole superpower, to a new and different situation that features, among other things, renewed great power status competition between Russia and China and challenges by these two countries and others to the US-led international order, that was established after the Second World War[1].

[1] Wolfgang Ischinger, MSC Chairman, *Munich Security Conference*, 15-17 February 2019, p. 1, available at https://www.securityconference.de/en/activities/munich-security-conference/munich-security-conference/msc-2019/ overview/, retrieved on 27 Mai 2019.

ROMANIAN MILITARY THINKING

The change of the international security environment was mainly made by using hybrid warfare. Deepening the analysis of the new international security environment, one can discover other emerging features, which create a much broader image of change and its genesis. It can be said that the world has changed in the recent years. The rise of the Islamic State (ISIS) and the resurgence of Russia are just a few examples. This fact shows that a broad strategic transition is ongoing and no different from those we have seen in history, after the end of major wars.

The general description of hybrid warfare is complemented by evaluation of parameters and capabilities of actors using this type of war, associated with target's vulnerabilities in the areas of interest and their overlap of means available and targeted effects. It follows that hybrid warfare is asymmetric and uses a wide range of instruments of power – military, diplomatic, economic and information ones, emphasising creativity, ambiguity, and the cognitive elements of war.

Now we can analyse and better understand the events in 2008 in Georgia, in December 2013, when China launched its land claim project in the South China Sea and in March 2014, when Russia illegally annexed Crimea and started to send its troops to support separatists in Donbass region, in eastern Ukraine, in 2014-2015.

The general description of hybrid warfare is complemented by evaluation of parameters and capabilities of actors using this type of war, associated with target's vulnerabilities in the areas of interest and their overlap of means available and targeted effects. It follows that hybrid warfare is asymmetric and uses a wide range of instruments of power – military, diplomatic, economic and information ones[2], emphasising creativity, ambiguity, and the cognitive elements of war.

However, all these place hybrid warfare outside the approach based on a war of attrition. If the instrument of power is similar to the response capacity of the target in that field, either qualitatively or quantitatively, then target vulnerabilities are exploited in order to degrade the capabilities.

An actor that uses hybrid warfare employs a number of specific actions to create effects and to escalate vertically and horizontally, synchronising political, economic, civil, information, cyber and military instruments of power. Therefore, an actor that uses hybrid war may escalate either vertically by increasing the intensity of one or more of the instruments of power or horizontally synchronising multiple

[2] Teodor Frunzeti, *Geostrategie*, Editura Centrului Tehnic-Editorial al Armatei, București, 2009, p. 51, apud Petre Duțu, Cristina Bogzeanu, *Interesele naționale și folosirea instrumentelor de putere națională pentru promovarea și apărea acestora. Cazul României*, Editura Universității Naționale de Apărare „Carol I", 2010, București, p. 14.

instruments of power, aiming at creating greater effects than those obtained only by escalating vertically.

A relevant element is that the aggressor uses simultaneously and in a synchronised manner various instruments of power in several dimensions and on multiple levels. This strategy allows the actor who uses hybrid warfare to take advantage of various political, economic, civil, informational, military, cyber means, available to create *synchronised attack packages* that are tailored specifically to the perceived vulnerabilities of the target system.

Although both state and non-state actors engage in a hybrid warfare, they vary greatly in terms of their means and actions. As a common point, all actors highlight the ability to synchronise various instruments of power against specific vulnerabilities to create linear and non-linear effects.

Although both state and non-state actors engage in a hybrid warfare, they vary greatly in terms of their means and actions. As a common point, all actors highlight the ability to synchronise various instruments of power against specific vulnerabilities to create linear and non-linear effects.

Generally, due to the relative novelty appearance, the knowledge of hybrid warfare is relatively low and therefore diminishes the ability to deter, respond, eliminate and counter that threat. The increase in the understanding of hybrid warfare by national policymakers, multinational security bodies and particularly by the armed forces leaders can develop effective possible solutions to counter this threat[3].

A conceptual approach to hybrid warfare can facilitate understanding and analysis of this type of war. The identification of specific elements of hybrid warfare and highlighting characteristics, stages, means, trigger and ongoing mode could consequently be used in identifying and analysing this type of conflict. Of paramount importance is that such an analysis should identify how the means of attack can be combined to form a synchronised attack system, adapted to target specific vulnerabilities.

Hostile actions typical to hybrid warfare are ambiguous, making it difficult for a state to identify, assign or publicly define the coercive use of force in the incipient phase. Ambiguity is used to complicate or undermine the decision-making process of a target state and is designed to make the response difficult. From a military perspective,

[3] Patrick J. Cullen & Erik Reichborn-Kjennerud, *"Understanding Hybrid Warfare", MCDC Countering Hybrid Warfare Project*, January 2017, p. 7, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf., retrieved on 27 May 2019.

the actions are designed specifically to be below the threshold of war and to delegitimise or make irrational actions to respond using military force.

Mitigation of hybrid warfare effects is favoured by the awareness on how actors using hybrid war adapt specific attacks on objectives, specific characteristic vulnerabilities established, belonging to the entire political, economic, civil, information, cyber and military spectrum.

The instruments of power used are determined by the capabilities of the actor that uses hybrid warfare and the perceived vulnerabilities of the target state, as well as the policy objectives and planned ways to achieve them. And as in all conflicts and wars, the character of hybrid warfare depends on the context also.

Russia has increased its emphasis on nuclear weapons, and other forms of unconventional capabilities and capacities specific to hyper warfare and hybrid warfare, to counter what Moscow considers to be the conventional military superiority of the USA and NATO.

Russia has increased its emphasis on nuclear weapons, and other forms of unconventional capabilities and capacities specific to hyper warfare and hybrid warfare, to counter what Moscow considers to be the conventional military superiority of the USA and NATO[4]. However, such thinking about the future war is not limited just to Russia. Radical Islamism groups such as al-Qaeda and ISIS are also exploring the use of technologies and strategies to penetrate Western open societies, to erode the protection of home security and undermine the social and political cohesion, upon which all security and defence policies in real democracies should be based. Russia's strategic goal of is to create a buffer zone to its south and west to obtain control over its high north, including the Arctic Circle and along its entire north border, which will likely form the new northeast corridor between Asia and Europe[5].

Moscow would also weaken the transatlantic link to force some European states enter a Russian sphere of influence and compel the rest to comply with the Russian strategic interests. In an ideal world for Kremlin, Russia's future war strategy would thus involve the eventual expulsion of USA, Canada and even the United Kingdom from Europe and its institutions, and the creation of a new European

[4] Jon S. Cleaves, *"Threats Tactics Report: Russia", TRADOC G-2 ACE Threats Integration*, version 1.1, October 2015, p. 5, available at https://community.apan.org/wg/tradoc-g2/ace-threats-integration/m/documents/211562, retrieved on 27 May 2019.

[5] *Ibid*, pp. 1-2.

security architecture, favourable to Russia. This new strategy is an old Russian method of action that can be sum up to leading war by using destabilisation, misinformation, strategic misleading, neutralisation and, if necessary, destruction.

It can be appreciated that there already is a new way of waging warfare. It is characterised by the following elements: achieving the goals with or without the employment of military force, by indirect actions, generating the constraint of enemy, politically, economically, informationally and psychologically, disorienting the political and military leadership of the target state, while disseminating discontent among the population, preparing the military response by deploying forces in the conflict zone, intensifying diplomatic pressure and propaganda on the international community by developing in secret and employing special operations forces, cyber-attacks and software effects, conducting large scale reconnaissance and subversion actions, supporting international opposition and acquiring and employing new weapons systems, using different types of weapons combined with the large-scale information effects, by entering enemy territory using simultaneous actions for the destruction of forces and targets in the depth of its territory, engaging precision weapons systems on large scale, extensively using special operations forces, robotic complexes and weapons based on nuclear power, destroying resistance centres with the help of artillery and airstrikes and landing of assault forces, seizing the territory using ground forces and establishing full control over target state[6].

Hybrid conflicts are aimed at increasing ambiguity, complicating the decision-making process and slowing coordination of effective responses. Due to these advantages for the aggressor, it is likely that this type of conflict will persist successfully in the future. The increasing reliance of Western populations on internet based social media makes diverse societies vulnerable to political manipulation via fake news. This is part of a new form of hybrid warfare that transcends civil-military division.

[6] Robert W. Kurz, *"Ukraine's Hidden Battlefield"*, *The Foreign Military Studies Office (FMSO)*, Fort Leavenworth, Kansas, 15.03.2017, pp. 94-95, available at https://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf, retrieved on 27 May 2019.

ROMANIAN MILITARY THINKING

Conceptual delimitations

Now the world faces multiple security challenges, simultaneously, from traditional state actors to trans-regional networks of sub-state groups, all taking advantage of rapid technological changes in the armaments field and the relatively slow response of the Western states[7]. Future conflicts will start faster, will last longer and will take place on a more challenging and technological battlefield. The complexity and rapid changes in key areas characterise the strategic environment today and are influenced by globalisation, unlimited and unrestricted access to technology and the rapid demographic changes.

Hybrid warfare, triggered by state or non-state actors, is usually adapted to remain below the obvious thresholds of detection and response, most often relying on speed, volume and omnipresence of digital technology, which facilitates the access to information. Some actors are increasingly using non-military means to achieve strategic and operational objectives, which were traditionally regarded purely as military goals.

Hybrid warfare, triggered by state or non-state actors, is usually adapted to remain below the obvious thresholds of detection and response, most often relying on speed, volume and omnipresence of digital technology, which facilitates the access to information. Some actors are increasingly using non-military means to achieve strategic and operational objectives, which traditionally were regarded purely as military goals.

Hybrid warfare can be described as synchronised use of multiple instruments of power adapted to specific vulnerabilities of full spectrum of social functions, in order to achieve synergy effects and to overcome the limitations specific to military[8].

Hybrid warfare incorporates a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and generalised coercion and criminal disorder[9]. It can be observed that the hybrid warfare is already widespread and widely used by state and non-state actors and is likely to evolve as a challenge that requires

[7] Strategic Concept for Defence and Security of the Members of the North Atlantic Treaty Organization, *Active Engagement, Modern Defence,* adopted by Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010, pp. 10-12, available at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, retrieved on 27 May 2019.

[8] Julio Miranda Calha, *"Hybrid Warfare: NATO's New Strategic Challenge?"*, Defence and Security Committee, 10 October 2015, pp. 4,7, available at https://www.nato-pa.int/documents?keys=HYBRID+WARFARE%3A+NATO%E2%80%99S+NEW+STRATEGIC+CHALLENGE%3F&field_year_value=All&sort_by=field_year_value, retrieved on 27 May 2019.

[9] Frank G. Hoffman, *"Conflict in the 21th Century: The Rise of Hybrid Wars"*, Potomac Institute for Policy Studies, December 2007, p. 8, available at http://www.potomacinstitute.org/events/23-publications/reports/1267-conflict-in-the-21st-century-the-rise-of-hybrid-wars, retrieved on 27 May 2019.

sustained efforts from states to acknowledge and counter the threat posed by this type of conflict.

romania2019.eu

To better understand the hybrid warfare, several related terms will be studied. Hybrid warfare combines features of conventional, irregular, and information warfare. It may also include economic and other forms of competition and contention imposed by the objectives to be achieved. Often used to describe information warfare, hybrid warfare also encompasses activities that fall outside of the information warfare range.

Grey zone warfare entails specific techniques different from traditional military field, to achieve their goals while denying those of its rivals by employing instruments of power that do not necessarily include the use of acknowledged regular military forces. These may involve state and non-state actors, and take place between the traditional state of wars and peacetime.

Unconventional warfare is the support of a foreign insurgency against its government or occupying power. It relies heavily on subversion through information and guerrilla warfare, and forces are often covert.

Unconventional warfare is the support of a foreign insurgency against its government or occupying power. It relies heavily on subversion through information and guerrilla warfare, and forces are often covert.

Information warfare involves the use and management of information to pursue a competitive advantage, including offensive and defensive efforts. According to Cold War diplomat George Kennan's definition, *political warfare is the employment of all the means at a nation's command, to achieve its national objectives*[10]. Such operations are both conventional overt and covert ones. They range from overt actions such as political alliances, economic measures, and official propaganda to covert operations such as clandestine support of hostile elements in the attacked state, psychological warfare and even encouragement of underground resistance in hostile state[11]. In this sense, information warfare is a form of political warfare, where targets include a nation state's government, military, private sector, and general population.

[10] George F. Kennan, "*On Organizing Political Warfare", National Security Council Policy Planning Staff document*, 30 April 1948, pp. 1-3, available at https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c, retrieved on 27 May 2019.

[11] *Ibid*, pp. 1-3.

Asymmetric warfare is fought between belligerents whose relative military power or whose strategy or tactics differ significantly. Information warfare can be a successful means of overcoming the disparity.

Soft power is, according to international relations scholar Joseph Nye, *"the ability to get what you want through attraction rather than coercion or payments"*[12]. This may involve the use of information with a positive spin in order to compel decisionmakers toward actions in one's own interests.

Baseline is a reference point to allow for the identification of indicators and events as well as measurement of variation away from that reference point. Establishing a standard baseline is a key part of the hybrid warfare self-assessment process and detection of hybrid war broke out.

Asymmetric warfare is fought between belligerents whose relative military power or whose strategy or tactics differ significantly. Information warfare can be a successful means of overcoming the disparity.

Critical functions are activities or operations distributed across the political, economic, social, information, cyber, infrastructure and military spectrum, the discontinuance of which would lead to the disruption of services that a working system, for example, a state, its society, or a subsection thereof, depends on. Critical functions can be broken down into a combination of actors, for example, individuals or organisations, infrastructures, for example, critical national power grids and processes, for example, legal, jurisdictional, technical and political.

Effects are a change of state of an entity as the result of actions against specific vulnerabilities of a target system.

Nonlinearity refers to unanticipated effects of hybrid warfare attacks that are not causally linear. They are the result of synergistic, simultaneous interaction, coordinated attacks of specific hybrid war attacks in which the whole is greater than the sum of their parts. Non-linear effects cannot always be predicted by the attacker or defender.

[12] Joseph S. Nye Jr., *Soft Power*, available at https://s3.amazonaws.com/academia.edu.documents/33300459/Soft_Power_Nye_1990.pdf?response-content-disposition=inline%3B%20filename%3DSoft_Power_Nye_1990.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190716%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190716T070935Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=8c3ecae4c0be3b05ede461dcceafc52c2bcd75be536849dcc4f25b0f308bf433, retrieved on 22.04.2019.

Synchronisation of means is the ability of a hybrid warfare actor to effectively coordinate the instruments of power (political, military, economic, cyber, civil and informational) to achieve the desired effects in both horizontal and vertical ways. The horizontal development of the hybrid conflict means the combined use of multiple instruments and means of power.

Indicators are measurable variables necessary to clearly and sufficiently identify/describe/represent/monitor a phenomenon in relation to a specific baseline.

Threshold is determining the magnitude or the intensity of a functional status, for example, the stress level of one's critical functions to be exceeded to achieve a specific status, for example, normal or crisis.

Vertical escalation is the intensified, amplified use of specific instruments and means of action by an actor. Vulnerabilities are personnel, activities, resources or processes within a potential target that are susceptible of being exploited or created by a potential adversary.

Synchronisation of means is the ability of a hybrid warfare actor to effectively coordinate the instruments of power (political, military, economic, cyber, civil and informational) to achieve the desired effects in both horizontal and vertical ways. The horizontal development of the hybrid conflict means the combined use of multiple instruments and means of power.

The impact of new technologies, and the interactions between them, is changing fast the nature, character and conduct of war. Hyper war implies an accelerated speed of conflict associated to a substantially shortened decision-making cycle. In these conditions, leading a war steadily and necessarily becomes more automated and part of a new escalation ladder that climbs from chaos to capitulation. The increasing reliance of western populations on internet based social media makes different societies vulnerable to political manipulation via fake news. This is basically part of a new form of hybrid warfare which transcends the civil military divide.

The end state of cyber warfare is the disruption of the information systems. Cyber-based civilian infrastructures, from healthcare to air transportation, will also be natural targets, adding a profound sense of uncertainty thus disrupting everyday life[13]. The threat of hyper

[13] Kimberly Amerson & Spencer B. Meredith III, *"The Future Operating Environment 2050: Chaos, Complexity and Competition"*, in *Small Wars Journal*, 31 July 2016, pp. 1-3, available at https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog1/posts/the-future-operating-environment-2050-chaos-complexity-and-competition, retrieved on 27 Mai 2019.

warfare, which is a conflict at the higher end of the military spectrum, would simply send a crushing message to the attacked state by those who have mastered it, namely that resistance is futile. One of the many dangers posed by such a hyper warfare, cyber warfare or hybrid warfare, is that it again renders plausible the once unimaginable idea of warfare in and between developed societies[14].

Traditional nuclear deterrence might also be considered as a stand-alone, increasingly obsolete stratagem of last resort. Indeed, deterrence, as it is currently conceived, will need to be rethought across the new spectrum of conflict if it is to remain a credible solution, while allied counteraction armed forces will need to become more capable across many domains: land, sea, air, space, cyber, intelligence, information, and, above all, knowledge.

Hybrid warfare uses techniques and tactics whose effects extend far beyond those specific to the military domain. Hybrid warfare is synchronised and systematic. The response should be the same. Each state is required to establish and set a permanent process of self-evaluation and analysis of threats and vulnerabilities. This process involves the concentration of intra and intergovernmental efforts to timely detect and counter hybrid threats.

Highlights of hybrid warfare

Hybrid warfare uses techniques and tactics whose effects extend far beyond those specific to the military domain. Hybrid warfare is synchronised and systematic. The response should be the same. Each state is required to establish and set a permanent process of self-evaluation and analysis of threats and vulnerabilities. This process involves the concentration of intra and intergovernmental efforts to timely detect and counter hybrid threats.

Hybrid threats are an international problem. The response should be the same. Nation states should coordinate within alliances, organisations, for a coherent approach with a view to detecting the aggression and preparing adequate response to a hybrid attack, according to their collective interests[15]. Russia has placed increased emphasis on nuclear weapons, and other forms of unconventional hybrid and hyper warfare capabilities and capacities, to counter what it believes to be NATO's conventional military superiority.

[14] Lord Jopling, *"Countering Russia's Hybrid Threats: An Update"*, Committee on the Civil Dimension Of Security (CDS), 1 October 2018, pp. 8-15, available at https://www.nato-pa.int/download-file?filename=sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf, retrieved on 27 May 2019.

[15] Matthew Rhodes & Ruta Buneviciute, *"Baltic and Central European Security after the Ukraine Crisis", Security Insights, George C. Marshall Center Publications,* pp. 2-3 available at https://www.marshallcenter.org/mcpublicweb/en/nav-fix-sec-insights/2184-art-pubs-sec-insights-11-full-en.html, retrieved on 27 May 2019.

While the armed forces focus on the military aspects, experts in civilian and private sector issues are required to conduct the analysis of unconventional risks specific to hybrid warfare. Self-assessment specific to a potential hybrid war target involves an ongoing national process to identify specific vulnerabilities to critical functions that belong to the entire social spectrum. On the other hand, violent extremist organisations pose an immediate threat to transregional security by coupling directly available technologies with extremist ideologies.

Thus, hybrid conflicts can employ military forces that assume a non-state identity, as Russia did in the Crimea, or may involve a violent extremist organisation fielding rudimentary combined arms capabilities, as ISIS did in Iraq and Syria. Hybrid conflicts may also comprise state and non-state actors working together towards common goals, employing a wide range of military means, as we saw in eastern Ukraine[16].

To have a clear idea about hybrid warfare, a pragmatic evaluation of key defining elements of hybrid warfare is required: **target state critical functions and vulnerabilities, synchronised use of a variety of means by the aggressor and exploitation of conflict horizontal escalation and, last, but not least, linear and nonlinear effects of the hybrid warfare**[17]. Finally, recommendations can be made, necessary for developing future solutions with a view to deterring, reducing, countering and combating hybrid war specific threats.

With regard to target state critical functions and vulnerabilities, we can mention as examples the exploitation of vulnerabilities, deep sectarian, ethnic and economic gaps in the Syrian society, which were exploited by both Iran and ISIS with a view to achieving their strategic objectives. All critical functions have vulnerabilities that a potential aggressor can take advantage of, according to its means. However, it is important to realise that not all vulnerabilities necessarily represent opportunities for an opponent to exploit.

Critical functions and vulnerabilities

With regard to the first category of elements, target state critical functions and vulnerabilities, we can mention as examples the exploitation of vulnerabilities, deep sectarian, ethnic and economic gaps in the Syrian society, which were exploited by both Iran and ISIS with a view to achieving their strategic objectives. All critical functions have vulnerabilities that a potential aggressor can take advantage of, according to its means. However, it is important to realise that not all

[16] Patrick J. Cullen & Erik Reichborn-Kjennerud, *op. cit*., pp. 11-16.

[17] Lord Jopling, *op. cit.*, pp. 3-8.

vulnerabilities necessarily represent opportunities for an opponent to exploit.

Alternatively, an opponent may choose not to exploit a specific vulnerability if it does not match his plans. In addition, vulnerabilities within critical functions can be enhanced by the aggressor by selecting the right time to trigger the attack, which may not be generally known by the system under attack, which can become aware of it only after it is underway. An example of exploiting vulnerabilities can be the action in May 2014, when the Russian hacker group CyberBerkut exploited cyber vulnerabilities, routers, software and hard drives of the Ukrainian National Election Commission to undermine the credibility of the elections. Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. *"Whoever becomes the leader in this sphere will become the leader of the world"*, as Russian President Putin stated in 2017[18].

The ability to synchronise both military and non-military means simultaneously within the same battlespace is considered a key characteristic of hybrid warfare. Synchronisation enables the hybrid warfare actor to escalate or de-escalate horizontally rather than just vertically, thus providing further options for the attacker. For example, by horizontal escalation, a hybrid warfare actor can keep the conflict below certain detection and response thresholds.

It follows that each state is required to consider its own critical functions and vulnerabilities graphics in relation to the military, political, economic, civil, cyber and information spectrum corresponding to the normal, crisis and emergency state.

Synchronisation

Regarding the second category, the ability to synchronise both military and non-military means simultaneously within the same battlespace is considered a key characteristic of hybrid warfare. Synchronisation enables the hybrid warfare actor to escalate or de-escalate horizontally rather than just vertically, thus providing further options for the attacker. For example, by horizontal escalation, a hybrid warfare actor can keep the conflict below certain detection and response thresholds.

By using this method, coercion can be used just as much, or even more, than if only one power instrument is escalated vertically. In other words, through horizontal escalation, a hybrid warfare actor

[18] John Allen, Philip M. Breedlove, Julian Lindley-French & George Zambellas, *"Future War NATO from Hybrid War to Hyperwar via Cyber War", Globsec NATO Adaption Initiative*, October 2017, p. 3, available at https://www.globsec.org/wp-content/uploads/2017/10/GNAI-Future-War-NATO-JLF-et-al.pdf, retrieved on 27 May 2019.

can create effects that are similar, or even greater, due to its capacity to multiply force, than by applying overt coercion through, for example, by using the political or military power instrument. A synchronisation example may be actions in autumn 2013, when Iran synchronised terrorist threats, cyber attacks and propaganda in order to deter foreign intervention in Syria or to influence the decision of the USA and allies[19].

Synchronisation also enables de-escalation of one or more instruments of power and alternating of means, while maintaining the overall level of escalation to a certain stage. Also, one instrument can be used for compensatory measures, while another may be used as a coercive measure.

Essentially, synchronisation and horizontal escalation provide the attacker with more options than when using only vertically synchronised escalation. The decisive element is that much of what takes place on the horizontal may be either ambiguous or hidden from observation, such as cyber operations, or conducted with unclear intent, such as investment in foreign critical infrastructure or uninterpretable as a hostile and aggressive act, for example instigation to non-violent protests.

Synchronisation and horizontal escalation provide the attacker with more options than when using only vertically synchronised escalation. The decisive element is that much of what takes place on the horizontal may be either ambiguous or hidden from observation, such as cyber operations, or conducted with unclear intent, such as investment in foreign critical infrastructure or uninterpretable as a hostile and aggressive act, for example instigation to non-violent protests.

Synchronisation has several advantages for the attacker. Among these, one can mention the ability to adapt means and vulnerabilities to effects, the ability to use constraint while acting below target detection thresholds, the ability to use constraint while acting under the threshold at which the target starts to react and the fact that it is easier to escalate and reduce the intensity simultaneously.

An example of synchronisation may be that, in parallel with the establishment of secret military training camps, ISIS set up missionary offices with a view to spreading the message of their religious organisation Salafi in local communities and to collecting information on all social structures. This information was used to reduce the effectiveness of political and military opposition.

The relative novelty of hybrid warfare lies in the ability of an aggressor to synchronise simultaneously multiple instruments of power

[19] Julio Miranda Calha, *op. cit.*, pp. 5-6.

and in the deliberate exploitation of creativity, ambiguity, confusion and cognitive elements of war in order to achieve the objectives[20]. Given this perspective, to understand the purpose, aims and intentions of a hybrid warfare user, it is required much more than a traditional threat analysis based on the aggressor's capabilities and intentions.

The traditional analysis of different instruments of power available for an opponent cannot predict how and to what extent these might be synchronised to create certain effects. Thus, the functional capabilities of a hybrid warfare adversary, although important, will not necessarily provide the needed and correct pieces of information to identify its course of action.

Effects and variety

The last element of analysis is represented by effects and variety. In hybrid warfare, the effects are understood as a change of state of an entity, which is the result of synchronised actions, properly adapted to the vulnerabilities of a specific system of the target state. The ability of a hybrid warfare actor to synchronise means against specific vulnerabilities in order to generate planned effects assumes that the target state planners cannot easily identify a direct causal chain of events. The more elements in the combination, the more difficult it is to establish the causality. An example in this respect is Ukraine abandoning negotiations with the EU, in November 2013, which generated the *Maidan* protests and resulted in the President being ousted from office, consequences exploited and capitalised on by Russia[21].

Actions specific to hybrid warfare do not necessarily lead to a standard result. Moreover, the same action can cause a different effect in a different context. While some forms of causality, second and third order effects respectively, might be visible in retrospect, non-linearity makes the analysis and especially the prediction based on prior examples extremely difficult. The advantage of non-linear effects is that they can be seen only after they manifested, being unpredictable

[20] Kimberly Amerson & Spencer B. Meredith III, *op. cit.*, pp. 1-3.
[21] Patrick J. Cullen & Erik Reichborn-Kjennerud, *op. cit.*, p. 13.

by definition. This also means that, the opponent cannot fully plan or control these effects. More importantly, the aggressor must be very flexible and prepared to capitalise on the effects of different actions as they occur.

A key aspect of the potential effects of hybrid war is the neutralisation caused by a series of synchronised events, difficult to detect or undetectable, operating below what would be conventionally a war. Moreover, usually, the disruption of normal state becomes obvious once the cumulative and non-linear effects begin to manifest.

Conclusions

Analysts have concluded that the international security environment is currently undergoing a shift in paradigm, the most relevant sign of change undoubtedly being Russia's seizure and annexation by force of Crimea in March 2014. This was the first occupation and annexation by force of a country's territory by another country in Europe after the Second World War[22]. Russia's resurgence and China's ongoing rise have created a new rivalry era for the superpower position and a corresponding requirement for NATO[23] to develop defence plans and programmes to meet these changes.

As described above, the attacks characteristic to hybrid warfare focus on specific vulnerabilities of a target, making them highly circumstantial. For a state to meet these threats, it needs a functional self-assessment system of its critical functions and vulnerabilities. Once critical functions and vulnerabilities are identified, it is necessary that thresholds are established to monitor changes in their functional status. Thresholds help to identify and define the severity of a hybrid warfare attack by pre-determining levels of normality, crisis or emergency, along with the magnitude or intensity that must be exceeded to move from one status level to the next.

An attack from a hybrid warfare actor using the military, political, economic, civil, cyber and information instruments of power may be disruptive, but not to an extent that a target is able to distinguish

An attack from a hybrid warfare actor using the military, political, economic, civil, cyber and information instruments of power may be disruptive, but not to an extent that a target is able to distinguish them from normal incidents. However, if these "incidents" happen many times or in other sectors simultaneously, the attack may cross detection thresholds due to the fact that synchronised actions can lead to cumulative and non-linear effects.

[22] Matthew Rhodes & G. Ruta Buneviciute, *op. cit.*, pp. 1-3.
[23] Lord Jopling, *op. cit.*, p. 1.

them from normal incidents. However, if these *"incidents"* happen many times or in other sectors simultaneously, the attack may cross detection thresholds due to the fact that synchronised actions can lead to cumulative and non-linear effects.

The above considerations lead to the conclusion that hybrid warfare does not perfectly fit into the traditional thinking, regarding the attack-phase. It does not necessarily evolve linearly through escalatory phases towards a strategically defined end state.

It should be emphasised that a hybrid warfare user may escalate and de-escalate simultaneously a conflict using different military, political, economic, civil, cyber and information instruments aimed at achieving planed objectives. For example, this tactic can also be used to hinder the development of multinational coalition against the hybrid war user.

Given the seriousness of hybrid threats, potential target states are required to develop national programmes for self-assessing, analysing and countering them. These programmes should direct the comprehensive intergovernmental efforts to identify, detect and respond to the threats posed by hybrid warfare.

Institutionalising a process to collect and disseminate information on threats and vulnerabilities of critical structures will enhance the efforts of early warning about hybrid war, will support the activities meant to resist to specific hybrid war actions and may even have a discouraging effect, because the conditions that could encourage an attack will be very limited. Finally, in principle, these efforts should be reproduced also at international and multinational level to intensify the efforts in the fight to counter the hybrid warfare.

Given the seriousness of hybrid threats, potential target states are required to develop national programmes for self-assessing, analysing and countering them. These programmes should direct the comprehensive intergovernmental efforts to identify, detect and respond to the threats posed by hybrid warfare.

Hybrid threats are an international problem – the answer would be the same. To do this, states are required to coordinate a coherent approach to identify, detect and respond effectively to hybrid war effects, according to their collective interests. In this context, the multinational environment – preferably using existing institutions and processes – should be effective to facilitate cooperation and collaboration across borders.

Hybrid warfare also creatively exploits our cognitive predisposition to enhance the military instrument of power, allowing the attacker

to intensify non-military means, and thus, at least in the beginning, to operate ambiguously, below the target's thresholds of detection and response. In practice, this can make it very difficult to identify the starting point of hybrid warfare. Moreover, it increases the possibility of a hybrid warfare actor to inflict significant damage on its opponent before they can respond to or possibly even detect a hybrid warfare attack. This strong and fluid element of ambiguity characteristic to hybrid warfare adds a new dimension to how coercion, aggression, conflict and war are to be understood. In this respect, the new geostrategic context and the technology boom, especially in the information environment, suggest the likelihood that this form of warfare continues to rapidly evolve into the future.

Hybrid warfare intentionally exploits ambiguity, creativity and common understanding of war in order to make the attacks as less visible as possible. This is owed to the fact that the actions of the aggressor will tailor to stay below certain detection and response thresholds, including international legal thresholds, thus hampering the decision-making process and making the reaction to such an attack more difficult.

Hybrid warfare intentionally exploits ambiguity, creativity and common understanding of war in order to make the attacks as less visible as possible[24]. This is owed to the fact that the actions of the aggressor will tailor to stay below certain detection and response thresholds, including international legal thresholds, thus hampering the decision-making process and making the reaction to such an attack more difficult.

Entirely different from the other conventional types of warfare, it is very difficult to notice a hybrid warfare campaign until it is already underway and causing destructive effect. In that phase, it is considered real and it has already jeopardised the capacity of the target state to defend itself. The issues described in this article provide the basis for expanding the traditional analysis of enemy-focused threat.

There is a big challenge for NATO to identify a possible hybrid attack as a rational reason for activating Article 5 of the Treaty of Washington, which regulates collective defence. NATO experts will need new ways to understand when an attack is initiated or in progress and to set a rapid action, to defence and counterattack, in the entire action range of hybrid defence warfare, thus using hybrid defence in response to a threat of the same type[25].

[24] Julio Miranda Calha, *op. cit.,* pp. 4, 7, 10.
[25] *Ibid,* pp. 4, 7.

BIBLIOGRAPHY

1. ***, *Strategic Concept for Defence and Security of the Members of the North Atlantic Treaty Organization, Active Engagement, Modern Defence*, NATO Lisbon Summit, 19-20 November 2010, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/ 20120214_strategic-concept-2010-eng.pdf.
2. John Allen, Philip M. Breedlove, Julian Lindley-French, George Zambellas, *Future War. NATO from Hybrid War to Hyperwar via Cyber War*, Globsec NATO Adaption Initiative, 2017, https://www.globsec.org/wp-content/uploads/2017/10/GNAI-Future-War-NATO-JLF-et-al.pdf.
3. Kimberly Amerson, Spencer B. Meredith III, *The Future Operating Environment 2050: Chaos, Complexity and Competition*, in *Small Wars Journal*, 2016.
4. Julio Miranda Calha, *Hybrid Warfare: NATO's New Strategic Challenge?*, Defense and Security Committee, 2015, https://www.nato-pa.int/documents?keys=HYBRID+ WARFARE%3A+NATO%E2%80%99S+NEW+STRATEGIC+CHALLENGE%3F&field_year_value=All&sort_by=field_year_value.
5. Jon S. Cleaves, *Threats Tactics Report: Russia*, TRADOC G-2 ACE Threats Integration, version 1.1, 2015.
6. Patrick J. Cullen, Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project Understanding Hybrid Warfare*, 2017, attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.
7. Frank G. Hoffman, *Conflict in the 21th Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, December 2007, http://www.potomacinstitute.org/events/23-publications/reports/1267-conflict-in-the-21st -century -the-rise-of-hybrid-wars.
8. Wolfgang Ischinger, MSC Chairman, *Munich Security Conference*, 15-17 February 2019, https://www.securityconference.de/en/activities/munich-securityconference/munich-security-conference/msc-2019/overview/.
9. Lord Jopling, *Countering Russia's Hybrid Threats: An Update*, Committee on the Civil Dimension of Security (CDS), 1 October 2018, https://www.nato-pa.int/downloadfile?filename=sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf.
10. George F. Kennan, *On Organizing Political Warfare*, National Security Council Policy Planning Staff document, 30 April 1948.
11. Robert W. Kurz, *Ukraine's Hidden Battlefield*, The Foreign Military Studies Office (FMSO), Fort Leavenworth, Kansas, 15.03.2017, https://docs.house.gov/meetings/AS/ AS26/20170315/ 105689/ HHRG-115-AS26-Wstate-ThomasT-20170315.pdf
12. Joseph Nye, *Soft Power*, in *Foreign Policy*, nr. 80 (Twentieth Anniversary), 1990, https://s3.amazonaws.com/academia.edu.documents/33300459/Soft_Power_Nye_1990.pdf?response-content-disposition=inline%3B%20filename%3DSoft_Power_Nye_1990.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190716%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190716T070935Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=8c3ecae4c0be3b05ede461dceafc52c2bcd75be536849dcc-4f25b0f308bf43313.
13. Matthew Rhodes, Ruta Buneviciute, *Baltic and Central European Security after the Ukraine Crisis*, Security Insights, George C. Marshall Center, Publications, 2015.

PARAMETERS FOR THE EUROPEAN UNION DEFENCE PLANNING PROCESS

Dragoş ILINCA

Institute for Political Studies on Defence and Military History, the Ministry of National Defence

The defence planning process has been one of the main areas where the European defence project progress has been substantially reflected. The evolution towards defining a European profile in managing the planning dimension associated with defence has been carried out in a short but very consistent timeframe, consistency deriving from the successively assumed transformations and innovations. The comprehensive character is the fundamental feature of the matrix in which planning aspects tend to be managed at the EU level. Overall, we talk about the coexistence of traditional aspects of force planning with prospective elements in the use of security and defence capabilities. Considering these coordinates, the profile of the planning process is an evolutionary approach, with a relevant conceptually-strategic foundation, through the Lisbon Treaty and the Global Security Strategy.

The present study aims at highlighting, on the one hand, the particular nature of the developments in the definition of planning procedures and, on the other hand, the specificities developed in this context. An important role is also given to valuing the elements of the future European defence planning model.

Keywords: European defence, battlegroups, capabilities, multinational cooperation, Helsinki.

English version by **Diana Cristiana LUPU**.

romania2019.eu

Introductory Ideas

The analysis of the defence planning process employed by the European Union is an issue insufficiently addressed in the literature. This situation can be attributed to the relatively early maturity of the European defence project, considering it has been developed for about two decades. Moreover, the intrinsic complexity of the subject should be taken into account in the context of the specific internal dynamics and the institutional features associated with the European defence dimension. The great number of involved structures as well as the member states strategic interaction in defining the objectives and priorities represent additional specific elements that influence the manifestation of the defence planning process developed in the European Union.

Viewed in a wider context, the analytical complexity associated with this theme is also highlighted by the particular political path taken in assuming the field of defence as a European Union sphere of activity. In this respect, the political circumstances that marked the development of the European Security and Defence Policy (ESDP) and the Common Security and Defence Policy (CSDP) have influenced the way in which the planning system used at the EU level has been developed. Thus, it can be noted a certain difficulty in identifying the traceability of the planning process evolution in the context of the general dynamics of the defence component.

The political circumstances that marked the development of the European Security and Defence Policy (ESDP) and the Common Security and Defence Policy (CSDP) have influenced the way in which the planning system used at the EU level has been developed. Thus, it can be noted a certain difficulty in identifying the traceability of the planning process evolution in the context of the general dynamics of the defence component.

Milestones and Institutional Interactions

The European defence cooperation formats started to emerge immediately after the end of the Second World War, being associated with Western Europe's concerns regarding security threats management in the geopolitical context of the time, dominated by the Cold War. Under such circumstances, the first decades marked the launch of initiatives aimed at strengthening the defence system to face a possible aggression by the Soviet Union coupled with the development of adequate formulas for Germany's participation

in the effort to ensure Europe's security. Such developments have two important components, namely the cooperation between Western European states and the development of transatlantic partnership, mainly by consolidating the USA commitment to European defence.

Institutionally, the concerns for the establishment of a European viable defence system generated the emergence of some multinational cooperation frameworks, under the auspices of the Western Union (1948-1954), the Western European Union (WEU – 1954-2009)[1] and the North Atlantic Treaty Organisation (NATO – April 1949). The common element was the goal of ensuring the member states collective defence in the event of an armed aggression, a fundamental principle politically assumed by the Brussels Treaty (17 March 1948, amended on 23 October 1954)[2] as well as by the North Atlantic Treaty (Washington, 4 April 1949)[3]. The implementation of the goal was reflected in the development of some frameworks intended for the integrated cooperation between the member states of those organisations, supported by certain defence resource planning processes. The focus was on the establishment of a comprehensive formula to manage the member states contribution to ensure the necessary conditions and capabilities to accomplish the missions deriving from the political commitments forming the basis of the mentioned organisations existence.

Institutionally, the concerns for the establishment of a European viable defence system generated the emergence of some multinational cooperation frameworks, under the auspices of the Western Union, the Western European Union and the North Atlantic Treaty Organisation. The common element was the goal of ensuring the member states collective defence in the event of an armed aggression, a fundamental principle politically assumed by the Brussels Treaty as well as by the North Atlantic Treaty.

1 The Western Union was established by France, Great Britain, Belgium, the Netherlands and Luxemburg signing the *Brussels Treaty* (17 March 1948). The approach was based on the Treaty of Alliance and Mutual Assistance signed by France and Great Britain in Dunkirk, on 4 March 1947. The Western Union continued to function, having poor results, up to 1954, when the failure in establishing the European Defence Community resulted in the necessity of re-evaluating the European cooperation in the field of defence. On 23 October 1954, the Brussels Treaty was amended, which led to the establishment of the Western European Union, a collective defence organisation too. It remained in function up to 1999, when it started to transfer its roles and responsibilities to the European Union. The Lisbon Treaty (2009) marked the completion of the process by including, within Art. 42.7 (Mutual Assistance Clause), the aspects relating to the signatory states collective defence.

2 The text of the Brussels Treaty, in Tony Insall, Patrick Salmon (ed.), *The Brussels and North Atlantic Treaties, 1947-1949*, in *Documents on British Foreign Policy Overseas*, series I, volume X, Whitehall History Publishing, 2015, pp. 455-459. For the changes in the Brussels Treaty made in 1954 see https://www.cvce.eu/content/publication/2003/11/26/7d182408-0ff6-432e-b793-0d1065ebe695/publishable_en.pdf, retrieved on 5 July 2019.

3 For the text of the North Atlantic Treaty see https://www.nato.int/cps/en/natolive/official_texts_17120.htm, retrieved on 5 July 2019.

Obviously, the first milestones in defining the defence planning system were generated in NATO context, evolving in synergy with the process of strengthening the integrated structures and functionalities of the North Atlantic Alliance. During this process, the principles, criteria and procedures proper to an integrated defence planning system were developed, which represented the main support instrument in coordinating the process of meeting NATO objectives. On the coordinates adopted at the North Atlantic Council meeting on 3-4 December 1970, certain benchmarks on the prospects of the Allied Planning Review process in the field of defence were established, thus enabling a long-term planning process[4]. It should be noted that the mentioned developments were part of the general context of the Cold War, the focus being on the force planning component, further outlined by the adoption, in the early '80s, of some specialised procedures.

The end of the Cold War and the diminishing of the threat of a conventional conflict led to a series of adjustments to the allied planning process. The *Strategic Concept* adopted at the NATO Washington Summit (24 April 1999) highlighted the member states interest in strengthening partnership policy in a wide range of areas[5], including the defence planning component. Moreover, the NATO Strasbourg-Kehl Summit (3-4 April 2009) promoted the necessity of addressing this aspect from a significantly different perspective by focusing on the comprehensive character of the planning process. Within the new approach it was aimed the consolidation of the qualitative aspects of the defence analysis process in order to enhance the member states contribution to the accomplishment of Allied missions. All the mentioned aspects got materialised in the formula of the NATO planning process adopted in 2009, the interaction between the planning domains thus becoming solid, including from the perspective of an enhanced connection between national planning systems.

The first milestones in defining the defence planning system were generated in NATO context, evolving in synergy with the process of strengthening the integrated structures and functionalities of the North Atlantic Alliance. During this process, the principles, criteria and procedures proper to an integrated defence planning system were developed, which represented the main support instrument in coordinating the process of meeting NATO objectives.

4 On this occasion, it was adopted a study on the issues the North Atlantic Alliance was confronted with in the '70s, based on which the Allied planning process premises were enhanced. For the Final Communique of the North Atlantic Council see https://www.nato.int/docu/comm/49-95/c701203a.htm, retrieved on 6 July 2019.

5 The set of domains considered for the cooperation with partner states within the Partnership for Peace, Mediterranean Dialogue, Ukraine and the Russian Federation included: training and exercises, interoperability, civil-military relations, development of concepts and doctrines, defence planning, crisis management, proliferation, cooperation in the field of armaments, participation in operations and operational planning, see https://www.nato.int/cps/en/natolive/official_texts_27433.htm, retrieved on 7 July 2019.

The typology of the Allied planning process includes the sequence of five stages focusing on:

- definition of guiding political elements (level of ambition);
- establishment of requirements by NATO strategic commanders;
- assignment of requirements and establishment of capability targets assumed by member states;
- facilitation of implementation by multinational initiatives and national efforts;
- assessment of the process of meeting the capability targets.

The typology of the Allied planning process includes the sequence of five stages focusing on: definition of guiding political elements (level of ambition); establishment of requirements by NATO strategic commanders; assignment of requirements and establishment of capability targets assumed by member states; facilitation of implementation by multinational initiatives and national efforts; assessment of the process of meeting the capability targets.

The planning horizon adopted following the introduction of the new planning model is, in essence, four years, providing a short, medium and long-term perspective of up to 20 years. Moreover, in streamlining the NATO planning process, 14 domains are considered, which provide the cooperation platform for the capability development in terms of: air and ballistic defence; air planning; civil emergency planning; C3I; cyber defence; armaments; force planning; intelligence; logistics; resources; medical field; science and technology; nuclear deterrence; standardisation and interoperability.

Introspection on the way in which the NATO planning process is structured represents an absolutely necessary element for the analysis of the system used at the level of the European Union. The system's genesis was, to a significant extent, related to the development of Allied planning procedures, which led to the adoption of joint frameworks, both on the conceptual dimension and on the practical level of implementation. The milestones associated with the mentioned developments were established by the Allied decisions in June 1996 relating to the European Security and Defence Identity within NATO[6], a conceptual approach meant to result in consolidating the European contribution to the security and defence effort.

The essence of the approach was the deeper cooperation between NATO and the WEU, by identifying certain capabilities to be used by the latter in conducting operations. In the context of defining a consolidated operational profile of the Western European Union, on the occasion of the Council of Ministers meeting held in Ostend on 19 November 1996, the decision was taken to strengthen the WEU involvement in the Allied planning process. One of the priority segments was to include in the NATO planning process illustrative

[6] Peter Duignan, *NATO: Its Past, Present and Future*, Hoover Institution Press, 2000, pp. 60-61.

scenarios for the range of missions undertaken by the WEU in the event of conducting operations[7]. The latter included, according to the Declaration adopted at the Council of Ministers meeting in Bonn, on 19 June 1992,the types of tasks the WEU could have achieved, such as: peacekeeping missions; crisis management missions, peacemaking included[8]. Mention should be made that, in the context of the close institutional relations between the WEU and the EU, following the Treaty of Maastricht (7 February 1992), *Petersberg tasks* were included in the Treaty of Amsterdam (entered into force on 1 May 1999), as they could be conducted in the context of the relations between the two organisations[9].

Development of the EU Planning Process Profile – Military Dimension

By the successive decisions regarding the consolidation of the cooperation relations between NATO and the WEU it started to develop what could be called the *European component of the planning process*. The increasingly close institutional connection between the WEU and the EU represented an additional instrument that strengthened the European character of that formula, exclusively centred on the inventory of *Petersberg tasks*, without considering the management of the implications deriving from the WEU Treaty in the field of defence. The decisions adopted at the Helsinki European Council (10-12 December 1999) would result in fundamental changes in the paradigm. The meeting coordinated by the Finnish Presidency of the Council of the European Union registered the political commitment to the first goal related to the development of the EU defence. The *Helsinki Headline Goal* (HLG 2003) stipulated the ability, up to 2003, to deploy within 60 days forces up to 50-60,000 personnel. They were to undertake the full range of *Petersberg tasks*, and could

The increasingly close institutional connection between the WEU and the EU represented an additional instrument that strengthened the European character of that formula, exclusively centred on the inventory of Petersberg tasks, without considering the management of the implications deriving from the WEU Treaty in the field of defence.

[7] Declaration of the WEU Council of Ministers in Ostend, on 19 November 1996. Text available at http://www.weu.int/documents/961119en.pdf, retrieved on 7 July 2019.

[8] The adoption of *Petersberg tasks* was added to the obligations regarding collective defence, according to the Brussels Treaty, amended in Paris, in 1954. For the text of the Petersberg Declaration, adopted by the Council of the WEU in June 1992, see http://www.weu.int/documents/920619peten.pdf, retrieved on 7 July 2019.

[9] Art. 17(2) (J7(2), For the text of the Amsterdam Treaty see https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_of_amsterdam_en.pdf, retrieved on 8 July 2019.

be kept in the theatre for at least one year[10]. To meet the goal, the adopted decisions were aimed at establishing the necessary structures at the EU level. They included the Political and Security Committee (PSC), consisting of ambassadorial-level representatives from all EU member states, meant to ensure the strategic coordination of the EU security and defence. The institutional military component to be established following the decisions adopted in Helsinki was primarily the Military Committee (EUMC), consisting of the member states chiefs of defence, responsible for supporting the decision-making process at the CDP level by providing military advice.

Moreover, the Military Committee could provide guidance for the activity of another structure, established following the decisions adopted in Helsinki, namely the European Union Military Staff (EUMS). Conceived as a multinational body integrated in the structure of the EU General Secretariat, the EUMS reunited military experts in the member states, the structure being responsible for supporting the European security and defence development process, from the perspective of the strategic planning associated with *Petersberg tasks* included.

Conceived as a multinational body integrated in the structure of the EU General Secretariat, the EUMS reunited military experts in the member states, the structure being responsible for supporting the European security and defence development process, from the perspective of the strategic planning associated with Petersberg tasks included.

The development of the EU institutional architecture in the field of planning represented one of the main aspects of the process of the European body general adaptation. Based on the decisions adopted at the Feira European Council (19-20 June 2000), it was established a working body exclusively meant to monitor the process of meeting the goal adopted in Helsinki. Under the coordination of the Military Committee, the Headline Goal Task Force (HTF) had to conduct the progress assessment process, focusing on the necessary capabilities to meet the HLG 2003[11].

The relevance of the Feira European Council should be also seen from the perspective of developing an assessment process meant to provide a comprehensive image of the results in meeting the goal assumed in December 1999. In this regard, the HTF ensured the organisation of the first Capability Commitment Conference (CCC), 20-21 November 2000. Structured in a manner that was relatively similar to NATO planning conferences, the meeting proposed an inventory

[10] Conclusions of the Helsinki European Council, in Maartje Rutten (ed.), *From St. Malo to Nice: European Defence: Core Documents*, Chaillot Paper 47, Western European Union Security Studies Institute, Paris, 2001, pp. 82-86.

[11] Santa Maria da Feira European Council, Presidency Conclusions, see https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00200-r1.en0.htm, retrieved on 8 July 2019.

of the capabilities that the member states could make available to meet the Helsinki goals. The use of this type of instrument would become a regular practice in the EU planning process, focusing on the assessment component.

Member states contributed, considering the CCC 2000, to meeting the HLG 2003, quantitatively, as follows: 100,000 – personnel; 400 combat aircraft; 100 ships[12]. The member states commitments within the CCC were integrated in a *Force Catalogue*, used, since then, as a planning instrument at the EU level.

Evidently, the actions derived from the decisions adopted in Helsinki outlined a distinct trajectory in the development of the EU planning process. From the constitutional point of view, planning prerequisites fit into a rather conventional vision, reflected in the 2003 HLG, the concrete expression of which was to be achieved through *Petersberg tasks*. Moreover, the military-classical paradigm under which the planning process evolved was strengthened by the coordination mechanism, in which the role of the EU military structures was decisive. In the context generated by the Commitment Conference in November 2000, the Nice European Council (7-9 December 2000) highlighted the necessity to establish a planning mechanism that allowed for the management of the HLG 2003-associated political decisions implementation process.

The actions derived from the decisions adopted in Helsinki outlined a distinct trajectory in the development of the EU planning process. From the constitutional point of view, planning prerequisites fit into a rather conventional vision, reflected in the 2003 HLG, the concrete expression of which was to be achieved through Petersberg tasks. Moreover, the military-classical paradigm under which the planning process evolved was strengthened by the coordination mechanism, in which the role of the EU military structures was decisive.

By the decision adopted by the heads of state and government, the Nice Summit advanced the strategic outline of the future defence planning framework, whose objectives were to strengthen the EU capability in terms of:

- Monitoring and facilitating the progress in implementing the assumed objectives, both quantitatively and qualitatively.
- Evaluating and, if necessary, reviewing the capability goals to meet the whole range of Petersberg tasks requirements.
- Developing a consistent process to include the commitments to the EU and the force goals agreed in the context of NATO Planning or the Partnership for Peace Planning and Review Process(PARP)[13].

[12] *Military Capabilities Commitment Declaration, 20 -21 November, 2000,* in Maartje Rutten (ed.), *From St. Malo to Nice: European Defence: Core Documents*, *op. cit.*, pp. 158-163. The CCC 2000 also included guidance on the need to develop an analysis process to identify deficiencies in the capabilities needed to operationalise the HLG 2003 (e.g. strategic airlift, C2, information, special forces, air supply etc.).

[13] The Nice European Council (7-9 December 2000), Presidency Report on ESDP, see https://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/00400-r1.%20ann.en0.htm, retrieved on 8 July 2019.

ROMANIAN MILITARY THINKING

Procedural Typology – Mechanism for the Development of Defence Capabilities

Under the auspices of the political framework agreed by the European Council on 28 February 2003, the Council of the EU adopted the decision to launch the *Capability Development Mechanism (CDM)*[14]. Through this instrument, the first elements of standardisation were introduced at the level of the European security and defence component, generating, at the same time, the methodology for the regular conduct of the planning process.

Under the auspices of the political framework agreed by the European Council on 28 February 2003, the Council of the EU adopted the decision to launch the Capability Development Mechanism (CDM). Through this instrument, the first elements of standardisation were introduced at the level of the European security and defence component, generating, at the same time, the methodology for the regular conduct of the planning process.

The first issue addressed was the **establishment of military requirements** to meet the EU's goals. Moreover, the member states contribution was considered. The stages of this procedural sequence, conducted through the interaction between the EUMC and the CSP, included:

❖ *Evaluation of the general objectives* assumed at the political level, from the perspective of identifying the progress achieved and analysing the impact of the developments in the security environment. In this context, the EUMC was required to provide the military approval regarding the capabilities necessary for meeting the political objectives, according to the decisions taken at the level of the European Council.

❖ *Review of military requirements*, managed in an integrated EUMC-HTF-EUMS framework, including by designing mission scenarios. This stage finality was the development of the *Requirements Catalogue*, through which a generic inventory of requirements, formulated with a certain degree of details in terms of quantitative and qualitative aspects, was included in the planning process. Given the importance of the mentioned document for guiding the whole planning process, the approval procedure entails the member states expressing agreement at the level of the European Council.

❖ *Making available national contributions*, where the main element was the integration, under the EUMC-HTF coordination, of the member states contributions, especially through the commitment conferences. The outcome of the process was the development of the *Force Catalogue* through which a comprehensive picture of the forces and capabilities that could be used for the EU-led operations was achieved. Like military requirements, the *Force Catalogue* is approved by the Council of the European Union.

The second component of the typology developed by the CDM is related to **monitoring and assessing progress** in meeting the goals, entailing the following stages:

❖ *Quantitative assessment* entails an iterative analysis process through which additional standardisation elements are introduced. The central role in this stage lies with the EUMS, which provides the interface with the member states to update their own contributions. The data on these issues are transmitted through a Headline Goal Questionnaire, developed synergistically with the similar instrument used for NATO Defence Planning Questionnaire.

❖ *Qualitative assessment* is conducted under the EUMC-HTF coordination and supported by the EUMS. The member states contributions are analysed from the perspective of a set of criteria aiming at: the degree of deployment, sustainability and interoperability. NATO's standards are used in this process, the responsibility for the assessment process being shared between member states (for forces) and the EU, through HTF (units with multinational potential, commands included).

❖ *Progress assessment* is conducted by the integrated analysis of the outcomes in the previous stages. These elements can be found in the *Progress Catalogue*.

romania2019.eu

Quantitative assessment entails an iterative analysis process through which additional standardisation elements are introduced. The central role in this stage lies with the EUMS, which provides the interface with the member states to update their own contributions. The data on these issues are transmitted through a Headline Goal Questionnaire, developed synergistically with the similar instrument used for NATO Defence Planning Questionnaire.

Level of Ambition

As it can be seen, the issue of reporting elements to guide the planning process at the EU level has significant peculiarities. In this respect, the decision taken at the Helsinki Summit corresponded to an initial stage of European cooperation in the field of defence, in which the 2003 HLG, *Petersberg tasks* included, represented the only benchmarks to guide the planning process. Thus, it can be mentioned a concrete political guidance deficit related to the strategic finality of the European defence dimension, more clarity on its parameters being necessary. With the development, in December 2003, of the first EU Security Strategy, the benchmarks needed to mature the defence commitment were advanced in connection with the evolutions in the international security environment. The Strategy also provided the necessary ingredients to formulate the EU's level of ambition in the field of security and defence, centred on the idea of a more active,

[14] Defining the EU Capability Development Mechanism (CDM), doc. 6805/26.02.2003, see https://data.consilium.europa.eu/doc/document/ST-6805-2003-INIT/en/pdf, retrieved on 9 July 2019.

more capable, more coherent and developed profile in cooperation with partners, objectives to which the defence dimension had a considerable contribution[15]. The main implications of the political commitment assumed through the Security Strategy that would contribute to the development of the level of ambition in the field of defence focused on:

❖ Strengthening the expeditionary capability under the European Security and Defence Policy, in the context of the multilateralism promoted by the EU in support of the UN actions.

❖ Developing the flexible profile and the operational mobility of forces, including through multinational cooperation frameworks between the member states to avoid duplication and to optimise the way in which budgetary resources are used.

❖ Initiating the process of reflection in relation to widening the scope of the missions assumed at the level of the security and defence dimension, including the support for combating terrorism and the reform of the security sector.

❖ Promoting an integrated approach in formulating the EU commitment, from the perspective of harmonising the different instruments developed for the military component included.

The EU level of ambition was enhanced through the adoption by the EU Council of a new objective for the ESDP development on 4 May 2004. Known as the 2010 Headline Goal (HLG 2010), it was a direct reflection of the interest for the qualitative strengthening of the EU defence approach.

On these coordinates, the EU level of ambition was enhanced through the adoption by the EU Council of a new objective for the ESDP development on 4 May 2004. Known as the 2010 Headline Goal (HLG 2010), it was a direct reflection of the interest for the qualitative strengthening of the EU defence approach[16]. Emphasis was placed on the development of crisis response through rapid response elements. According to the agreed parameters, it was intended to establish, by 2007, *battlegroups* (1,500 soldiers), intended to be force structures to be used as independent units or in connection with a greater EU

[15] The Security Strategy adopted during the meeting of the Council of the European Union on 12-13 December 2003, was developed under the coordination of the High Representative for Foreign Affairs and Security Policy, Javier Solana. For the text of the strategy, *A Secure Europe in a Better World*, see https://www.cvce.eu/en/obj/european_security_strategy_a_secure_europe_in_a_better_world_brussels_12_december_2003-en-1df262f2-260c-486f-b414-dbf8dc112b6b.html, retrieved on 9 July 2019, also in Antonio Missiroli (ed.), *European Defence: Core Documents. From Copenhagen to Brussels*, Chaillot Papers, no. 67, vol. IV, Institute for Security Studies, European Union, Paris, 2003, pp. 324-334.

[16] The promotion of the project for the battlegroups establishment in the HLG 2010 context was conducted through the French-British-German Non-Paper, in early February 2004. It also included the experience acquired following the conduct of the first EU autonomous operational commitment, Operation Artemis, in RD Congo (May-September 2003).

commitment. Their development was based on the structure of an infantry battalion, strengthened by logistical and combat support capabilities. The adoption of the mentioned objective was in line with the goals of the Security Strategy, in particular in terms of the degree of deployment and interoperability of the forces made available by the member states. In this respect, it was aimed the deployment of *battlegroups* within maximum 10 days from the decision to launch the operation, which could be kept in the theatre for up to 120 days.

On these coordinates, the effects of the adoption of the new goal at the level of the defence planning process were substantial. From a conceptual perspective, the decision brought the planning dimension much closer to the operational aspects of the EU commitment, approach visible by capitalising on the lessons learned from the operations. Secondly, the adoption of the 2010 HLG promoted an integrated approach, also reflected in the planning process, from the perspective of a synergistic use of civilian and military capabilities in formulating the EU operational commitments.

Moreover, the HLG 2010 associated decision resulted in including rapid response capabilities in the planning process, coupled with a particular focus on the availability of command and control elements necessary to conduct operations employing such capabilities. From this perspective, it was established to develop certain benchmarks relating to the degree of deployability, interoperability and multinational training of the forces made available by member states. In support of the planning process optimisation, the segment relating to the development of the *Progress Catalogue* was backed by the conduct of a supplementary analytical exercise, oriented on four directions: available capabilities – shortfalls – operational risks – prioritisation[17].

The HLG 2010 associated decision resulted in including rapid response capabilities in the planning process, coupled with a particular focus on the availability of command and control elements necessary to conduct operations employing such capabilities. From this perspective, it was established to develop certain benchmarks relating to the degree of deployability, interoperability and multinational training of the forces made available by member states.

The declaration of the battlegroups full operational capability (1 January 2007)[18] allowed for outlining a level of ambition in a classical-operational matrix. Thus, the Council of the EU on 11-12 December 2008 set as objectives for the development of the EU

[17] *Scrutinize – Assessment – Evaluation – Prioritization Procedure*.

[18] Confirmed by the Conclusion of the Council of the European Union on 21-22 June 2017 (doc.). As far as operational planning was concerned, on 1 January 2017, there were in stand-by two battlegroups in Germany – the Netherlands – Finland, and in France – Belgium formats.

capability to carry out military operational commitments, planning and simultaneous command:

- Two major stabilisation and reconstruction operations, supported by 10,000 troops, for about two years;
- Two rapid response operations having a set period of time and using, *inter alia*, *battlegroups*;
- An evacuation operation for European citizens (in less than 10 days);
- An air police/denial mission;
- A civilian-military operation of up to 90 days[19].

To meet this level of ambition, there were used the available forces and capabilities generated by the member states contribution following the adoption of the HLG 2003 and the HLG 2010. As it can be seen, all the elements of the level of ambition reflected the objectives of the Security Strategy, based on the missions assumed by the EU by integrating the Western European Union functions.

Development of an Integrated Planning System

The particular significance of the HLG 2010 also resided in approaching the issue of the capability shortfalls identified following the planning process. Up to that moment, the Capability Development Mechanism was focused on the military planning component, the area of shortfalls being treated separately. The Brussels/Laeken European Council (14-15 December 2001) adopted the decision to initiate a consolidated analysis process related to capability shortfalls. In this regard, it was launched the European Capability Action Plan (ECAP)[20], an initiative having an ad-hoc character, meant to identify some solutions for each type of shortfall identified during the planning process conducted through the CDM. ECAP activities, under the EUMC coordination, were conducted following a common methodology for all battlegroups. The data identified through the CDM were structured relating to 38 capability shortfalls, presented during the defence ministers meeting in May 2003. Evidently, the identified solutions entailed the development of a constant assessment process, supported

The particular significance of the HLG 2010 also resided in approaching the issue of the capability shortfalls identified following the planning process. Up to that moment, the Capability Development Mechanism was focused on the military planning component, the area of shortfalls being treated separately. The Brussels / Laeken European Council (14-15 December 2001) adopted the decision to initiate a consolidated analysis process related to capability shortfalls. In this regard, it was launched the European Capability Action Plan.

[19] Presidency Conclusions, Brussels European Council, 11-12 December 2008, see http://data.consilium.europa.eu/doc/document/ST-17271-2008-INIT/en/pdf, retrieved on 10 July 2019.

[20] Laeken European Council, Presidency Report, in Maartje Rutten, *From Nice to Laeken: European Defence: Core Documents*, vol. II, Security Studies Institute, European Union, Paris, 2002, pp. 133-136.

by an adequate institutional framework allowing for timely capitalising on member states contribution. From this perspective, the ECAP could not be a sustainable solution for the process management.

The new approach included the establishment of the European Defence Agency (EDA)[21], whose main responsibility was to manage the process of developing the European defence capabilities, in compliance with the political objectives assumed for the development of the European Security and Defence Policy. In this context, the EDA developed the project for a new initiative, the Capability Development Plan (CDP), including the parameters of an integrated defence planning framework. The CDP was intended to ensure the management of all the components associated with the ESDP development at the level of a joint mechanism able to provide the milestones for the conduct of the European defence project and, subsequently, to highlight the priorities on which the project should focus. From this perspective, the new initiative main objectives were:

❖ To connect the European defence capability process with the strategic trends in the security environment.

❖ To identify the capability development priorities, from the standpoint of the ESDP goals and the military level of ambition. The mentioned component was also aimed at monitoring the way in which the collective targets set for the development of defence cooperation were met[22].

❖ To support the cooperation process among the member states, focusing on jointly using the capabilities.

❖ To develop industrial research and cooperation at the EU level.

Without being necessarily assimilated to a supranational planning process, the CDP would be, from that moment on, the backbone of the EU defence planning to be updated every five years. The first Capability Development Plan was adopted at the level of the EDA Steering Committee held in the format of defence ministers on 12 March 2011.

Without being necessarily assimilated to a supranational planning process, the CDP would be, from that moment on, the backbone of the EU defence planning to be updated every five years. The first Capability Development Plan was adopted at the level of the EDA Steering Committee held in the format of defence ministers on 12 March 2011. The conceptual developmental approach was based on the identification of some planning areas that were assessed as essential for conducting missions within the ESDP context.

[21] Formalised through the Council Decision (CFSP)2015/1835 on 12 October 2015, Official Journal of European Union, L266/13.10.2015, pp. 55-74.

[22] On the occasion of the EDA Steering Committee meeting, within the defence ministers meeting on 19 November 2007, the collective defence spending targets were adopted. In this regard, it was agreed the modality of the member states defence spending, outlined to meet the following objectives: procurement – 20% of the total defence spending; joint procurement programmes – 35% of the total procurement spending; research-development-technologies – 2%; collaborative projects in the field of R&T – 20% of the total spending in the fields, see https://www.eda.europa.eu/info-hub/defence-data-portal/benchmarks, retrieved on 12 July 2019.

The conceptual developmental approach was based on the identification of some planning areas that were assessed as essential for conducting missions within the ESDP context. In this regard, the chosen domains were related to the following capabilities: command and control; intelligence; engagement; protection; deployment; support[23]. Similar to NATO planning areas, the mentioned domains represented the main benchmarks of the EU planning process, to which progress report was related.

The way in which the CDP was developed was exclusively based on the interaction between the member states and the European institutions responsible for defence. In the context of integrated approach, all existing data and pieces of information were used in the planning process.The results obtained following their processing and the dialogue between the member states were structured considering the components presented below:

The way in which the CDP was developed was exclusively based on the interaction between the member states and the European institutions responsible for defence. In the context of integrated approach, all existing data and pieces of information were used in the planning process.

❖ *Strand A* (coordinated by the EUMC) – elements having relevance in the short term (five years), provided through the Capability Development Mechanism, associated with the process of monitoring progress in meeting goals.

❖ *Strand B* (coordinated by the EDA) – aspects derived from the analysis of trends in the long term (2025+) and the assessment of the impact on capability requirements.

❖ *Strand C* (managed by the EDA) – analysis elements, in the medium term (5-15 years), regarding the projects and programmes conducted at the member states level, including from the perspective of their impact on capability requirements. The data management was achieved through a database (CODABA).

❖ *Strand D* (coordinated by the EUMC) – relevant aspects derived from the lessons learned following the EU operational commitments.

In the mentioned context, it was identified a set of priorities having high relevance for the European capability development process, including: improvised explosive devices (C-IED); medical support; intelligence, surveillance and reconnaissance; enhanced helicopter availability; cyber defence; multinational logistic support; ESDP information exchange; air transport management – strategic&tactic; fuel and energy; mobility assurance[24].

[23] EDA Report 2011, European Defence Agency, Brussels, 2011.

[24] For the inventory of the priorities established within the first CDP exercise see https://www.eda.europa.eu/what-we-do/our-current-priorities/strategies/Capabilities, retrieved on 10 July 2019.

The trend to strengthen the CDP integratory character for the evolution of the European defence cooperation significantly increased in the years to follow, against the background of the structural developments that followed the adoption of the Lisbon Treaty (13 December 2007). The innovations thus introduced resulted in outlining a new conceptual-institutional framework for the development of the Common Security and Defence Policy. Therefore, the scope of *Petersberg tasks* was widened by introducing new tasks associated to joint disarmament operations, military advice and assistance, post-conflict stabilisation[25]. Moreover, the new treaty included provisions related to the implementation of the solidarity principle in the field of security and defence in member states, from the perspective of the mutual defence clause in the event a EU member state is a victim of armed aggression (Art. 42.7), or of the solidarity clause for civilian emergency situations (Art. 222)[26].

The trend to strengthen the CDP integratory character for the evolution of the European defence cooperation significantly increased in the years to follow, against the background of the structural developments that followed the adoption of the Lisbon Treaty (13 December 2007). The innovations thus introduced resulted in outlining a new conceptual-institutional framework for the development of the Common Security and Defence Policy. Therefore, the scope of Petersberg tasks was widened by introducing new tasks associated to joint disarmament operations, military advice and assistance, post-conflict stabilisation.

The deepening of the strategic framework associated with the development of the security and defence dimension underwent substantial changes through the adoption of the new *Global Strategy for the European Union* (EUGS, June 2016). Promoting a global vision of the EU responsibilities in the context of the current security challenges, the EUGS stipulated the important role played by strengthening the European defence capabilities, considered from a multidisciplinary perspective. In this context, it was highlighted the necessity of common approaches in the field of defence, by integrating the concrete aims of the defence capability development process in relation to industry as well as research and development[27]. In the same vein, the EUGS mentioned a new level of ambition in the EU defence and security, formulated in a conceptual paradigm, essentially defined on three main coordinates: the EU capacity to respond to conflicts and external crises the moment they break out; the partner states strengthened capability in the contemporary security context; the protection of the EU and its citizens.

[25] Art. 43, for the text of the Lisbon Treaty see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2007:306:TOC, retrieved on 9 July 2019.

[26] The text of the Lisbon Treaty, in Official Journal of the European Union, C306/17.12.2019.

[27] *Shared Vision, Common Actions: A Stronger Europe. A Global Strategy for European Union's Foreign and Security Policy* (June 2016), see http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, retrieved on 12 July 2019.

To implement the new strategic vision, in the period following the EUGS adoption, there were launched certain initiatives regarding the development of the European Permanent Structured Cooperation (PESCO) in the field of defence as well as the financial support for the domain. At the end of 2017 it was launched the PESCO implementation process[28], an initiative meant to support some concrete projects related to capability development. Moreover, at the beginning of 2019, the European Parliament adopted the Defence Fund Regulation[29], an instrument expected to be functional within the EU multiannual financial framework (2021-2027), contributing to the financial support for the capability projects that will be developed at the EU level. In addition, in order to enhance European cooperation in the field of planning, the Council of the EU approved (November 2016) the initiation of a Coordinated Annual Review on Defence (CARD), to allow for the development, on a voluntary basis, of an effective capability shortfalls management system. Starting from the priorities established in the Capability Development Plan, the CARD process is aimed at deepening the synergy among national approaches, the cooperation development and the consolidation of coherence in defence spending at the member states level[30].

To implement the new strategic vision, in the period following the EUGS adoption, there were launched certain initiatives regarding the development of the European Permanent Structured Cooperation in the field of defence as well as the financial support for the domain. At the end of 2017 it was launched the PESCO implementation process, an initiative meant to support some concrete projects related to capability development.

The elements that guide the activities conducted under the mentioned initiatives are found on the agenda developed based on the priorities established by the CDP. Responding to the significant developments in the dynamics of the European security and defence dimension as well as in the security environment, at the end of June 2018, a new Capability Development Plan was adopted.

[28] According to the provision of the Treaty on the EU (Art. 42 and Protocol 10 of the Treaty), the Decision of the Council of the EU CFSP2017/2315 on 11 December 2017 launched the Permanent Structured Cooperation in which 25 member states participate. Up to now, the initiative has made significant progress by the adoption of 34 capability projects. For details regarding PESCO developments see https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en, retrieved on 12 July 2019.

[29] Through the European Defence Fund 13 billion Euro will be channelled into capability development projects (8.9 billion) and defence-related research (4.1 billion). For the text of the Regulation see https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-eu-defence-fund-regulation_en.pdf, retrieved on 12 July 2019.

[30] Based on the decision of the Council of the EU, between 2017 and 2018, the CARD trial was developed. In 2019 the initiative became operable under the EDA coordination. For further details regarding the preparation phase seehttps://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card), retrieved on 12 July 2019.

Starting from the priorities formulated by the member states within the framework of the dialogue with the EDA, coupled with the results of the analysis processes conducted at institutional level, the CDP 2018 advanced a new set of priorities, developed from the perspective of identifying the optimal formulas to cover the capability shortfalls, focusing on the operational dimension. Moreover, they were aligned with the EUGS goals, being compliant with the member states perceptions regarding the developments in the security environment. From this perspective, the inventory of the priorities agreed by the new Capability Development Plan includes: capabilities for operations in the context of cyber warfare; space communications and information services; information superiority; land combat capabilities; logistical and medical support capabilities; naval mobility; submarine control; air superiority; air mobility; integration of air capabilities in the aviation sector; relevant capabilities to meet the EU level of ambition[31].

Conclusions

As it can be seen, the evolution of the defence planning process at the EU level covers a relatively short period of time, indicating the low maturity level of the European profile in this field. In this context, the traceability of this dimension of the European defence project represents a challenge in itself, considering the complex modality to accommodate the diverse developments occurred during the past two decades.

The evolution of the defence planning process at the EU level covers a relatively short period of time, indicating the low maturity level of the European profile in this field. In this context, the traceability of this dimension of the European defence project represents a challenge in itself, considering the complex modality to accommodate the diverse developments occurred during the past two decades.

However, it should be noted that the incremental development of this field has resulted in the emergence of some specificities as far as the future defence planning model used by the European Union is concerned. The particularity mainly derives from the intrinsic nature of the European body that has generated the interdisciplinary cooperation frameworks between different institutional actors having responsibilities in the field of defence. Moreover, the progress marked by the introduction of the Capability Development Plan indicates the planning process transformation from a system focused on engagement scenarios to a comprehensive approach, in which the main role is held by the adaptability of the types of capabilities to the uncertainties in the security environment.

[31] For further details see https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f, retrieved on 12 July 2019.

Secondly, the planning process, successively defined by an asymmetrical series of documents and decisions, tends to exceed the classical framework of the domain by articulating an integrated system. As it has been proved in the past years, special focus is placed on the interaction between the classical planning and the industrial component in the European Union, from the perspective of the practical options it can provide to cover the shortfalls. The synergy of the mentioned elements contributes to strengthening the comprehensive defence character of the planning process, which generates both opportunities and significant challenges for the member states. In this regard, it should be mentioned the substantial role played by national contributions in guiding and supporting the planning process, in all its components, creating the premises for a comprehensive approach to defining priorities.

The planning process, successively defined by an asymmetrical series of documents and decisions, tends to exceed the classical framework of the domain by articulating an integrated system. As it has been proved in the past years, special focus is placed on the interaction between the classical planning and the industrial component in the European Union, from the perspective of the practical options it can provide to cover the shortfalls.

BIBLIOGRAPHY

1. Peter Duignan, *NATO: Its Past, Present and Future*, Hoover Institution Press, 2000.
2. Tony Insall, Salmon, Patrick (ed.), *The Brussels and North Atlantic Treaties, 1947-1949*, in *Documents on British Foreign Policy Overseas*, series I, vol. X, Whitehall History Publishing, 2015.
3. Antonio Missiroli (ed.), *European Defence: Core Documents. From Copenhagen to Brussels*, Chaillot Papers, no.67, vol. IV, Institute for Security Studies, Paris, 2003.
4. Maartje Rutten, *From Nice to Laeken: European Defence: Core Documents,* vol. II, Security Studies Institute, Paris, 2002.
5. Maartje Rutten (ed.), *From St. Malo to Nice: European Defence: Core Documents*, Chaillot Paper, nr. 47, Western European Union Security Studies Institute, Paris, 2001.

WEBOGRAPHY

1. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00200-r1.en0.htm.
2. https://data.consilium.europa.eu/doc/document/ST-6805-2003-INIT/en/pdf.
3. https://www.cvce.eu/content/publication/2003/11/26/7d182408-0ff6-432e-b793-0d1065ebe695/publishable_en.pdf.
4. https://www.cvce.eu/en/obj/european_security_strategy_a_secure_europe_in_a_better_world_brussels_12_december_2003-en-1df262f2-260c-486f-b414-dbf8dc112b6b.html.
5. https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f,
6. https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_of_amsterdam_en.pdf.
7. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.
8. https://www.nato.int/cps/en/natolive/official_texts_27433.htm.
9. http://www.weu.int/documents/961119en.pdf.

PERMANENT STRUCTURED COOPERATION – A SMALL STEP FOR THE EUROPEAN MILITARY-POLITICAL INTEGRATION?

Dacian DUNA, PhD

Lecturer, International Studies and Contemporary History Department, Faculty of History and Philosophy, Babeș-Bolyai University, Cluj-Napoca, doctoral studies in International Relations and European Studies

Raul-Ciprian DĂNCUȚĂ, PhD

Assistant Professor, Security Studies Programmes, Faculty of History and Philosophy, Babeș-Bolyai University, Cluj-Napoca, doctoral studies in International Relations and European Studies

The present paper is aimed at providing a nuanced assessment of the well-known initiative in the field of political-military cooperation between the EU member states established in 2017 – Permanent Structured Cooperation (PESCO), in compliance with the requirements of the Lisbon Treaty decision-making framework.

The article highlights PESCO evolution, subsuming it under a set of similar initiatives that have got materialised in the European construction process, such as EUROCORPS or EU Battle Groups. Each and every step of integration, starting even from intergovernmental cooperation mechanisms, can provide long-term benefits, generating the necessary synergies to complete the European integration process. In this respect, it could be mentioned the establishment of the common European Union armed forces, a step forward towards the establishment of the European federation. However, the main obstacle for the small steps of integration to be followed by the big step is represented as always by the political will.

Keywords: integration, cooperation, institutions, EU, PESCO, CSDP.

English version by **Diana Cristiana LUPU**.

Introduction

In a domestic and international political climate that is relatively hostile to the European Union, it is difficult to identify any positive steps that have the potential to lead Europe towards the achievement of its major political desiderata, having at the core, almost as a chimera, the idea of the European federation. However, there are still hopes for the European Union, among many failed projects and contested reactions, from Eurosceptic domestic political forces, as well as from international rivals such as Russia, China or even the United States. Small steps towards integration, starting from the structured cooperation mechanisms initiated between the member states, assisted by the Community institutions, could create, in a time horizon still difficult to discern, the necessary impetus for Europe to achieve its destiny, namely a union of federative type. It is not the purpose of this study to demonstrate the viability of such a construction, but it seems reasonable for countries that have long left their historical conflicts aside in favour of an increasingly broad and fruitful collaboration to aspire to a regional integration. Moreover, the concentration of world power at the hands of some regional superpowers is an almost unquestionable fact, which makes small European countries second-hand powers in the new international order. However, what we are attempting to assess is whether initiatives such as PESCO can give a real *"impetus"* to the political-military integration or, on the contrary, will be added to the list of notable failures, alongside the old European Defence Community or the Constitutional Treaty.

Small steps towards integration, starting from the structured cooperation mechanisms initiated between the member states, assisted by the Community institutions, could create, in a time horizon still difficult to discern, the necessary impetus for Europe to achieve its destiny, namely a union of federative type.

Despite the emergence and intensification of some hotbeds of Euroscepticism, not only in Western but also in Eastern Europe (the Visegrad group), European citizens seem to express their trust for the European Union. The results of the latest Eurobarometer confirm the fact that the confidence in the EU has got consolidated following Brexit, 42% of respondents declaring their support for the Union[1].

[1] See *Standard Eurobarometer 89*, spring, 2018, web version: file:///C:/Users/Asus/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/eb_89_first_en%20(1).pdf, retrieved on 14.07.2019.

The result does not appear impressive. Mention should be made that the confidence in the European institutions and in the European Union has dramatically decreased following the sovereign debt crisis in 2009, it being indirectly linked to losing confidence in national institutions and not to exclusively blaming the Union for the disastrous situation in those years[2]. Moreover, the Eurobarometer in the spring of 2018 (no. 89) indicates the fact that the main concerns at European level are connected to security: the issue of immigrants, which is related to societal security, holds the first position, while terrorism, which affects human security, holds the second position[3]. Economy and environment, which, in turn, have an indubitable security component, are *"ranked"* immediately after the already mentioned issues.

As it is indicated by the results of Eurobarometer, which assesses the European public opinion, as well as by the debates related to the elections for the European Parliament and even by the results of the elections, European citizens do not want less Europe, as predicted by Eurosceptics and right-wing populists, but a Europe able to resolve their problems and to ensure more security as well as an environment conductive to the development of public and private life.

As it is indicated by the results of Eurobarometer, which assesses the European public opinion, as well as by the debates related to the elections for the European Parliament and even by the results of the elections, European citizens do not want less Europe, as predicted by Eurosceptics and right-wing populists, but a Europe able to resolve their problems and to ensure more security as well as an environment conductive to the development of public and private life. We express our reservations about the nation states capacity to solve all the mentioned problems in a strictly national framework[4]. If the European Union can be made a *scapegoat* for the failure in meeting the objectives considered fundamental for the European citizen, the member states can be equally blamed for not implementing the strategic decisions adopted at the Community level. From the *European Union Internal Security Strategy* (reviewed in 2015) to the *European Union Global Strategy* (2016) and even the *Permanent Structured Cooperation* (2017), we notice, in most cases, the initiation of certain mechanisms to implement and even monitor the implementation, but not completed projects. In addition, it is also noteworthy that it took a decade from the Lisbon Treaty adoption to the PESCO initiation, which indicates the fragility of consensus at the Community level and the maintenance of quite obvious nationalistic tendencies, which reduce the ability to make optimal decisions in favour of certain minimalist compromise.

The slow recovery of the European economy after the sovereign debts crisis has allowed for the partial shift of focus from the domestic issues to the European and international agenda. However, it is also due to external *"stimuli"*. In our opinion, the evolutions occurred within the framework of the European Union Common Foreign and Security Policy in the past years (especially after June 2016) have had complex causes including Brexit (23 June 2016), the adoption of the *Global Strategy for the European Union Foreign and Security Policy* (28 June 2016), the continuation of the Russian Federation aggressive policy towards the Union eastern limes[5], as well as the context generated by the election of the Trump Administration in the USA (20 January 2017). In the background, the issues of immigrants and of terrorism from Islamist sources have continued to generate waves of deep concern at the domestic and community level, overexploited by the traditional mass media and the social networks on the Internet. All these factors, combined with the pressures exercised by certain Community institutions such as the Commission, the President of the European Council, or the High Representative for Foreign Affairs and Security Policy, indirectly caused changes in the decision-making climate in member states, which finally resulted in assuming initiatives having a larger scope.

Cooperation in the Field of Security and Defence – Major EU Project

Although it seems a reactive decision related to the vote in the UK Referendum for leaving the Union, the adoption of the *Global Strategy* was preceded by years of debates and negotiations between

[2] Anna Brosius, Erika J. van Elsas and Claes H. de Vrees, *Trust in the European Union: Effects of the Information Environment*, in *European Journal of Communication*, 2019, vol. 34(1), pp. 57-73.

[3] *Standard Eurobarometer 89*.

[4] The *"Chinese wall"* policy did not prevent the danger of barbarian invasions in China. In the age of globalisation, it is much more difficult to defend the borders of a country by employing internal means only, considering the cross-border threats that *"volatilize"* borders, such as climate change, global economy evolution, cyber-attacks and even the refugee issue. The costs of refusing to cooperate with the others are prohibitive for the states that have to allocate huge sums of money to maintain a high living standard for their citizens, considering they are increasingly demanding as far as the political class is concerned. The results of the latest elections in Europe attest to this fact.

[5] Even if there is certain stabilisation of the conflict area in Donbass (Eastern Ukraine), the Russian Federation has continued to reaffirm the dominant position in the Black Sea, strengthening the already significant military potential in Crimea, a province annexed on 18 March 2014 (an act not accepted by the international community). The actions of Russia are doubled by a rhetoric that is very hostile to the West, in general, and to the North Atlantic Alliance, in particular, as well as by the focus of propaganda and disinformation on the states at the eastern limes of NATO and the EU.

member states. Its adoption was imposed by the new realities in the international security environment, doubled by the limitations of the *EU Security Strategy*, a document in force since 2003.

With reference to the Brexit role of catalyst, which triggered, in our opinion, rapid and exceptional developments in the area of the EU foreign affairs and common security, we can state that, among all the EU common policies, security and defence not only provide a very good visibility but also bring into debate the old issue of ceding some elements of national sovereignty in favour of the decision made at the European Union level. The European Union has actually needed, starting in late 2016, powerful signs of unity and European integration strengthening[6]. In this regard, it is not at all accidental the choice regarding the subtitle of the *EU Global Strategy – Shared Vision, Common Action: A Stronger Europe*, a title that enunciates the main theme of united Europe actions starting in June 2016, as well as one that signifies the neuralgic point, namely the European integration strengthening.

The first step taken by the EU leaders was the adoption, during the Warsaw NATO Summit (8-9 July 2016), of a joint declaration on increasing practical cooperation in the field of security. In essence, the document stipulated strengthened cooperation between the EU and NATO to combat hybrid threats, operational cooperation at sea and on migration, coordination on cyber security and defence, development of coherent, complementary and interoperable defence capabilities.

The first step taken by the EU leaders was the adoption, during the Warsaw NATO Summit (8-9 July 2016), of a joint declaration on increasing practical cooperation in the field of security. In essence, the document stipulated strengthened cooperation between the EU and NATO to combat hybrid threats, operational cooperation at sea and on migration, coordination on cyber security and defence, development of coherent, complementary and interoperable defence capabilities, facilitation of stronger defence industry and greater defence research, and better coordination on military exercises[7]. The fact that the declaration was signed by the European Council President, by NATO Secretary General and by the European Commission President, as well as by the US President signifies the transfer to the leaders of the main European executive institutions of the role of the Union representatives in the field of security and defence, in relation to the most important institutional companion, NATO, to the detriment of the nation states that are members of both organisations. Thus, both the intergovernmental level (through the European Council) and

[6] It should be acknowledged here that the UK used to be, unfortunately, one of the bastions of opposition to any initiative that could weaken NATO authority over the European security and the member states sovereignty.

[7] European Council, *EU-NATO Joint Declaration*, 08.07.2016, https://www.consilium.europa.eu/en/meetings/international-summit/2016/07/08-09/ retrieved on 15.07.2019.

the supranational one (through the European Commission) in the European Union decision-making chain were satisfied.

In November 2016, the foreign affairs and defence ministers adopted the Implementation Plan on Security and Defence under the EU Global Strategy[8], through which the level of ambition and the way forward on the future development of the EU security and defence policy were established. The actions proposed to achieve the assumed level of ambition include: setting priorities for capability development; enhancing cooperation between member states; adjusting structures, tools and working methods; developing partnerships. The objectives were accompanied by examples of concrete results: more efficient defence spending; more rapid response if need arises (crisis or emergency situations); joint planning and conduct of non-combat missions; possibility of developing a new permanent structured cooperation[9].

The European Commission adopted, on 30 November 2016, the European Defence Action Plan. The most important proposal made by the Commission in this Plan may be the establishment of the European Defence Fund, conceived to include two financing directions, complementary but different in terms of their juridical structure and budgetary source.

The European Commission adopted, on 30 November 2016, the European Defence Action Plan[10]. The most important proposal made by the Commission in this Plan may be the establishment of the European Defence Fund, conceived to include two financing directions, complementary but different in terms of their juridical structure and budgetary source. The first one would focus on defence research and the second one would act as a financial instrument meant to allow the participant member states to procure certain assets in common in order to reduce costs[11]. It should be highlighted that, although it does not play a direct role in the decision-making process within CFSP-CSDP (through the Lisbon Treaty), the European Commission manages, through the financial levers, to achieve a central position in implementing the decisions made by the European Council and by the Council of the European Union, fact that can only enhances the level of integration even in the mentioned domains, given the supranational character of the Commission. On 15 December 2016,

[8] Foreign Affairs Council, EU, 14-15/11/2016. *"The Implementation Plan on Security and Defence"* under the *EU Global Strategy*, see https://www.consilium.europa.eu/en/meetings/fac/2016/11/14-15/, retrieved on 15.07.2019

[9] *Idem*, *EU Global Strategy: Implementation Plan on Security and Defence*, see https://www.consilium.europa.eu/en/infographics/eu-global-strategy/, retrieved on 15.07.2019.

[10] *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions*, *European Defence Action Plan*, Brussels, 30.11.2016, COM(2016) 950 final.

[11] It is noted a revitalisation of the concept of *Pooling and Sharing*.

the European Defence Action Plan was adopted by the European Council. Mention should be made that there was apparently consensus between the three European institutions involved in the field of defence, almost certainly due to permanent intermediary negotiations between these institutions and member states. This way, the unity of vision is supported, and progress is not made until all the appeals that could throw the Community approach into derision are resolved.

PESCO Implementation and Operationalisation

The Permanent Structured Cooperation was stipulated in the Lisbon Treaty against the background of the compromises made by the member states that resulted in the signing of the treaty. It represents a unique procedure within the CSDP, a policy normally associated with unanimity, aimed at spurring defence integration.

The *Permanent Structured Cooperation* was stipulated in the Lisbon Treaty against the background of the compromises made by the member states that resulted in the signing of the treaty. It represents a unique procedure within the CSDP, a policy normally associated with unanimity, aimed at spurring defence integration. It is a variant of enhanced cooperation, introduced in the Treaty of Nice, in 2000. PESCO stipulates that the member states *"whose military capabilities fulfil higher criteria, and which have made more binding commitments to one another in this area, shall establish a permanent structured cooperation within the EU framework"* (Art. 28A.6)[12]. The procedure is mentioned in Protocol no. 10 of the Lisbon Treaty. It was invoked, considering reasons partially explained in the present paper, only in 2017.

The reactivation of the clauses of the Lisbon Treaty on common defence and security was only a consequence of the developments in both the international security environment and the Union. Internally, the EU political support reached alarmingly low levels during 2007-2016, the whole European construction being in danger of rejection by European citizens. Brexit is an indirect consequence of these trends. Internationally, the EU became the target of increasingly revisionist international actors, being almost the only one normative actor, except for a more contested organisation – the UN. Even the USA, the EU traditional ally, started to criticise both the Union and globalism, through the voice of President Donald Trump.

On 13 November 2017, the ministers of 23 member states signed a common notification regarding their involvement in permanent structured cooperation. Reserved in the beginning, Ireland and Portugal joined the initiative, completing the number of the countries that wanted development in the field of PESCO[13] (EU 25). The notification included PESCO[14] principles, the focus being on the fact that the initiative is an ambitious European juridical framework, mandatory and comprehensive for the investment in the EU territory and citizens security and defence. In Annexe 2 of the notification, it was presented the list of *"common ambitious and mandatory commitments"*, the member states approved to assume. There are actually 20 principles among which we highlight those related to increasing defence budgets in compliance with the investment in military procurement amounting at least 20% of the budget. In the final annexe of the notification the rules of PESCO Governance were established. It is important to mention that the decision-making process remains at the level of member states, which assume the obligation to ensure the transparency of actions for non-participatory states.

The implementation of the permanent structured cooperation was to be completed by the Council of the European Union on 11 December 2017. 25 out of 28 member states participated, except for Denmark (which, through the Treaty, refused to participate in the CSDP), the UK (which had to comply with the new internal political realities related to Brexit) and Malta.

The implementation of the permanent structured cooperation was to be completed by the Council of the European Union on 11 December 2017. 25 out of 28 member states participated, except for Denmark (which, through the Treaty, refused to participate in the CSDP), the UK (which had to comply with the new internal political realities related to Brexit) and Malta[15]. On that occasion, it was also adopted a list of 17 projects to be developed within PESCO. The following domains were aimed at: European Medical Command; European Secure Software defined Radio (ESSOR); Network of Logistic Hubs in Europe and Support to Operations; Military Mobility; European Union Training Mission Competence Centre (EU TMCC); European Training Certificate Training for European Armies; Energy Operational (EOF); Deployable Military Disaster Relief Capability Package; Maritime (semi-) Autonomous Systems for Mine Countermeasures; Harbour and Maritime Surveillance and Protection (HARMSPRO); Upgrade of Maritime, Surveillance Systems; Cyber Threats and Incident Response Information Sharing Platform; Cyber Rapid Response Teams and Mutual Assistance in Cyber Security; Strategic Command

[12] Art. 42 – *Provisions regarding the Common Security and Defence Policy*, Para. (3), the European Union Treaty enhanced version, in *The European Union Official Journal*, C 83/27, 30.3.2010.

[13] Denmark defined its position not to participate in the CSDP through the Treaty (invoking the principle of constructive abstention), and the UK excluded itself through voting Brexit.

[14] Notification on Permanent Structured Cooperation (PESCO) to the Council and to the High Representative of the Union for Foreign Affairs and Security Policy, Annexe 1, see https://www.consilium.europa.eu/media/31511/171113-pesco-notification.pdf, retrieved on 15.07.2019.

[15] Malta adopted the *"wait and see"* attitude.

and Control (C2) System for CSDP Missions and Operations; Armoured Infantry Fighting Vehicle/Amphibious Assault Vehicle/Light Armoured Vehicle; Indirect Fire Support; EUFOR Crisis Response Operation Core (EUFOR CROC)[16].

From the simple enumeration of these objectives we can notice the broad scope of the projects intended to be developed within PESCO. They were meant to bridge the technological gap and to reduce the dependence on the United States and, moreover, to help the states having less technologized armed forces in setting up capabilities to cope with the new realities in the battlefield.

The roadmap was intended to strategically orient the stages in meeting commitments. It included a calendar for the review and assessment process of the national implementation plans as well as a calendar for achieving agreement over certain possible projects. Mention should be made that the member states voluntarily assume national terms and obligations in the field of defence, which allow them to subsequently participate in joint programmes.

As it was expected, the next Council, that on 6 March 2018, adopted a recommendation related to the roadmap for PESCO implementation[17]. The roadmap was intended to strategically orient the stages in meeting commitments. It included a calendar for the review and assessment process of the national implementation plans as well as a calendar for achieving agreement over certain possible projects. Mention should be made that the member states voluntarily assume national terms and obligations in the field of defence, which allow them to subsequently participate in joint programmes. However, it can be noted the absence, from the list of projects, of the great procurement projects for military assets (aviation, navy, tanks), aspect that allows for the member states to continue their procurement policies in compliance with national strategies and interests. It can be interpreted as a concession made to the US ally, a top provider for the member states armed forces.

A year after PESCO implementation, it is noticed a significant increase in defence budgets by 3.3% in 2018, estimated by 4.6% in 2019, as well as the increase in joint investment in the field of defence. Moreover, it should be appreciated the fact that the member states national defence planning is increasingly assisted by the EU means, initiatives and instruments in the field[18].

[16] European Council, 14-15 December 2017, *Permanent Structured Cooperation (PESCO)* first collaborative PESCO projects – Overview, pp. 1-6, Brussels, 12 December 2017, see https://www.consilium.europa.eu/media/32123/h-pec-tusk-summits-171214-15-euco-background-final-euco-brief-factsheet-overview.pdf, retrieved on 15.07.2019.

[17] The EU Council, Council Recommendation of PESCO Implementation Roadmap, 6558/1/18, Brussels, 6 March 2018, see http://data.consilium.europa.eu/doc/document/ST-6588-2018-REV-1/ro/pdf, retrieved on 15.07.2019.

[18] The EU Council, Press Release, 14/05/2019, *Defence Cooperation:The Council Assesses Progress Made in the Framework of PESCO after the First Year of Implementation*, see https://www.consilium.europa.eu/ro/press/press-releases/2019/05/14/defence-cooperation-council-assesses-progress-made-in-the-framework-of-pesco-after-first-year-of-implementation/, retrieved on 15.07.2019.

Certainly, this perspective can be considered an optimist one. However, not all PESCO-related approaches generated the same general enthusiasm. The French President, Emmanuel Macron, relaunched an almost impossible challenge some time ago: in November 2018, in a radio broadcast, he supported, in a manner reminding of the Pleven Plan[19], the establishment of a European army to respond to Russia challenge in the East as well as to spur the EU emancipation in relation to the USA. The most virulent reaction was, as expected, that of President Trump. Moreover, Macron project was rejected by some European partners already involved in PESCO or by the not involved member states (on the top of the list was the UK, still an EU member state). On the other hand, it was saluted by the partner of France in European affairs, Germany (represented by Angela Merkel, whose interactions with President Trump were not very positive), as well as by the European Commission.

The project of common European armed forces is not a new one (the eldest example in this regard is the European Defence Community in the early ’50s). The President of the European Commission, Jean-Claude Juncker, originated from Luxembourg, supported it in 2015 in response to Russia aggressiveness at the EU eastern limes. An article written by Pierre Haroche, an *Euobserver* (online newspaper) journalist, illustrated the interests behind relaunching the idea of common European armed forces, Macron project: *“For the European Commission, for example, the goal has largely been to legitimise an incursion into the field of defence, which has long been the exclusive domain of member states. That incursion started recently with the launch of the European Defence Fund. For the German government, the goal was to demonstrate its commitment to European integration, from a political rather than a military perspective. (…). As for Macron, he is seeking to underline his European commitment a few months before EU elections, on which he is investing quite a bit”*[20]. Paradoxically, even Eurosceptic conservative leaders, such as Orban or Zeman, declared in favour of Macron project[21].

The project of common European armed forces is not a new one (the eldest example in this regard is the European Defence Community in the early ’50s). The President of the European Commission, Jean-Claude Juncker, originated from Luxembourg, supported it in 2015 in response to Russia aggressiveness at the EU eastern limes. An article written by Pierre Haroche, an Euobserver (online newspaper) journalist, illustrated the interests behind relaunching the idea of common European armed forces, Macron project.

[19] French Prime Minister, René Pleven, suggested, in 1950, a series of radical measures for the Western Union common defence, including European armed forces and a European Defence Minister.

[20] Pierre Haroche, *“Macron’s “European Army”: Why Is Everyone Talking about It?”,* in *Euobserver*, Paris, 14 November 2018, see https://euobserver.com/opinion/143372, retrieved on 16.07.2019.

[21] *Ibidem.*

ROMANIAN MILITARY THINKING

PESCO Implications for the European Construction

From the perspective of the role played by PESCO in further European integration, we should note that the European defence policy is much more than European integration. The intergovernmental cooperation that lies at the basis of CSDP and, implicitly, of PESCO somehow contradicts the realistic basis of the states in which national security and defence are, in essence, the very reason for the state existence. We can thus deduce that it is less likely for the member states to accept losing control over national security issues in the process of integration[22]. Moreover, intergovernmentalism tends to provide too much support for the importance of negotiations among member states leading to signing common decisions or treaties, and less support for the impact the agreements can have in the intermediary period (between two treaties)[23].

From the perspective of the role played by PESCO in further European integration, we should note that the European defence policy is much more than European integration. The intergovernmental cooperation that lies at the basis of CSDP and, implicitly, of PESCO somehow contradicts the realistic basis of the states in which national security and defence are, in essence, the very reason for the state existence. We can thus deduce that it is less likely for the member states to accept losing control over national security issues in the process of integration.

The transfer of the national security responsibility to entities that are currently perceived as supranational (EU) seems to be an impossible approach if the collective mindset and political discourse remain unchanged. Ultimately, it is easy to notice that any type of European policy generates more integration, through the significant number of people directly involved or benefiting from that particular policy. Therefore, our justification that PESCO can be a new engine of European integration. Mention should be made that supranationalism also plays an important part. Both the European Commission and the European Parliament are called to express or to actively contribute to implementing PESCO. The role of the PESCO Secretariat, which comes from European institutions of supranational source (the European External Action Service, the European Defence Agency, the General Secretariat of the European Council) and, in particular, the High Representative for Foreign Affairs and Security Policy, a personality at the heart of European foreign policy, should not be neglected either.

It should be also mentioned that the functionalist and neo-functionalist theories of European integration highlight the relationship between individual/collective interests and integration. The supporters of neo-functionalist theories overestimate the role of elites, disregarding the civil society, while functionalists support a European construction having as goal the federal state, considering the main role held by European institutions in meeting this goal[24]. We appreciate that the error of the functionalist theory is related to underestimating the importance of the nation state that, as it can be noted, continues to play the main role in the European construction. In the process of PESCO operationalisation, the member states have played the essential part, the directions for action being ultimately the result of the negotiations conducted by their representatives within responsible European institutions.

romania2019.eu

The functionalist and neo-functionalist theories of European integration highlight the relationship between individual/collective interests and integration. The supporters of neo-functionalist theories overestimate the role of elites, disregarding the civil society, while functionalists support a European construction having as goal the federal state, considering the main role held by European institutions in meeting this goal.

With strict reference to the role of military issues in stimulating the process of integration, we find that, although the realistic basis of the sovereign state is represented by national security and defence[25], the military factor has played a role of catalyst for the establishment of federative or confederative states. The most eloquent examples in this respect are, in our opinion, the USA and the USSR. It is true that integration followed certain bloody military conflicts (the War of Secession and the Civil War, after the Bolshevik Revolution). However, the question arises if European wars, or, better to say, their spectrum, could play the same role? It is to be reminded not only that the European integration has resulted in almost 70 years of peace in Western Europe but also that the wars in the Balkans, Transnistria, Georgia or Ukraine continue to haunt Eastern Europe.

Conclusions

Looking back at the evolution of the negotiations that ultimately led to the establishment and operationalisation of PESCO, we notice the reaction of European decision-makers to the pressure exerted by the international security environment, as well as to the new European realities marked by the referendum related to the United Kingdom leaving the Union. Contrary to the general perception regarding the slowness with which decisions are adopted in the UE, we can state that, in the particular mentioned case, although the reaction speed

[22] C.J. Bickerton, B. Irondelle and A. Menon, *Security Co-operation beyond the Nation- State: The EU's Common Security and Defence Policy*, in *Journal of Common Market Studies*, no. 49(1), 2011, p. 8.

[23] Geoffrey Garrett, George Tsebelis, *An Institutional Critique of Intergovernmentalism*, in *International Organization*, vol. 50, no. 2, spring, 1996, p. 269.

[24] Arie M. Kacowicz, *Regionalism, Globalization, and Nationalism*, Working Paper 262, December 1998, in *The Hele Kellog Institute for International Studies*, editor Caroline Domingo, p. 26, apud Adrian Ivan, *Guvernanță și teorii ale integrării în Uniunea Europeană*, course notes, Centre for European Studies, *"Alexandru Ioan Cuza"* University, Iași, p. 36.

[25] Hans J. Morgenthau, *Politica între națiuni. Lupta pentru putere și lupta pentru pace*, Editura Polirom, Iași, 2007, pp. 151-188.

ROMANIAN MILITARY THINKING

was not spectacular in terms of time, it was carefully considered, the European approach being preceded by intense negotiations among the member states, facilitated and stimulated by Community institutions such as the High Representative, the European Council (represented by the President), the Council of the European Union and the European Commission. However, the decisions regarding security and defence could be adopted, even in the context of maintaining the CSDP specific voting system[26]. Given the scope, we can state that the European decision has met the unprecedented challenge Europe has to face, European leaders managing to convey a clear and firm message regarding the decision to preserve and consolidate the European project. Moreover, there have been met both the levels and the methods related to the Union functioning, namely the intergovernmental (represented by the European Council and the Council of the European Union) and the supranational one (represented by the European Commission).

The succinct presentation of the developments within the CSDP, which focus on PESCO implementation, highlights, in our opinion, the effort made by the European leadership to cope with the new realities in the field of security: occupation of the Crimean Peninsula by the Russian Federation, Brexit, the reorientation of the US foreign policy.

The succinct presentation of the developments within the CSDP, which focus on PESCO implementation, highlights, in our opinion, the effort made by the European leadership to cope with the new realities in the field of security: occupation of the Crimean Peninsula by the Russian Federation, Brexit, the reorientation of the US foreign policy. The rapidity with which declarations, recommendations, roadmaps and action plans have been adopted indicates the acknowledgement of the danger generated by the referendum for the UK leaving the Union, attempting to prevent the propagation of a domino-type phenomenon, which could result in the EU dissolution. Ultimately, the evolution of the international system changes the profile of the threats and vulnerabilities that define the issue of security[27]. This fact leads to an increase in awareness of non-military threats, which get more influent, without considering the decrease in awareness of military threats.

With regard to the question *What are we doing?* and, especially, *How are we doing*? to strengthen the Union, European leaders have chosen defence and security as the pillars to consolidate the European project. Evidently, in the above described context, they used to represent the most emotional and controversial domains. However, they have also generated sufficient arguments for strengthening the European unity.

[26] Unanimity Principle.

[27] Barry Buzan, *Popoarele, statele şi teama*, Editura Cartier, Chişinău, 2000, pp. 368-370.

romania2019.eu

PESCO thus highlights, in the context of awareness of vulnerabilities, risks and threats to security, that the rational political decision takes precedence over nationalist and populist slippages. It still remains the question whether PESCO will become an engine of strengthening the European unity and the European project, in general. It is yet difficult to answer this question. However, we appreciate that, alongside the security objectives assumed under the *EU Global Strategy*, PESCO, as part of the EU security and defence strategy, could become an engine of integration. The 34 projects already assumed within PESCO will bring Europeans closer to each other, will generate common values, even if they are mainly material ones, and will raise the awareness, for the European citizens, that together they are stronger and better prepared to meet the current security challenges.

PESCO thus highlights, in the context of awareness of vulnerabilities, risks and threats to security, that the rational political decision takes precedence over nationalist and populist slippages. It still remains the question whether PESCO will become an engine of strengthening the European unity and the European project, in general. It is yet difficult to answer this question.

We can conclude that the temptation to nominally assume the European construction project is still visible in the European leaders, for reasons related to personal prestige, as well as for electoral reasons. Apparently, there are the small projects triggered by initiatives such as PESCO that better represent the certainties of continuing the project of thorough integration. They seem to deeply erode, in a neo-functionalist manner, the last barriers imposed by states to prevent the European federalisation. Learning from the cooperation within PESCO, many stakeholders, be they individuals or institutions, will better acknowledge the benefits of political-military integration in the long run. International organisations have demonstrated their extraordinary ability to find levers of cooperation rather than of reciprocal annihilation, in this case being considered the EU-NATO relation. Therefore, we do not believe in the fatalistic prediction of the opponents of the common European armed forces according to which their establishment will mean NATO dissolution. In fact, all common projects continue as long as there are shared principles, values and interests.

BIBLIOGRAPHY

1. ***, European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions*, *European Defence Action Plan*, Brussels, 30.11.2016, COM(2016) 950 final.

2. ***, EU Council, *Press Release 14/05/2019, Cooperation in Defence: The Council assessed progress made in the framework of Permanent Structured Cooperation (PESCO) after its first year of implementation*, https://www.consilium.europa.eu/ro/press/press-releases/2019/05/14/defence-cooperation-council-assesses-progress-made-in-the-framework-of-pesco-after-first-year-of-implementation/.
3. ***, EU Council, *Council Conclusions on Security and Defence in the Context of the EU Global Strategy*, Brussels, 19 November 2018, http://data.consilium.europa.eu/doc/document/ST-13978-2018-INIT/ro/pdf.
4. ***, EU Council, *Council Recommendations regarding PESCO Implementation Roadmap*, 6558/1/18, Brussels, 6 March 2018, http://data.consilium.europa.eu/doc/document/ST-6588-2018-REV-1/ro/pdf.
5. ***, Council of the EU, *Notification on Permanent Structured Cooperation (PESCO) to the Council and to the High Representative of the Union for Foreign Affairs and Security Policy*, Annexe 1, https://www.consilium.europa.eu/media/31511/171113-pesco-notification.pdf.
6. ***, European Council, *EU-NATO Joint Declaration*, 08.07.2016, https://www.consilium.europa.eu/en/meetings/international-summit/2016/07/08-09/.
7. ***, European Council, *Joint Declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg*, European Council, 08.07.2016, https://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf.
8. ***, European Council, *Meeting (22 and 23 June 2017) – Conclusions*, Brussels, 23 June 2017, EUCO 8/17, https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf.
9. ***, European Council, 14-15 December 2017, *Permanent Structured Cooperation (PESCO) First Collaborative PESCO Projects – Overview*, pp. 1-6, Brussels, 12 December 2017, https://www.consilium.europa.eu/media/32123/h-pec-tusk-summits-171214-15-euco-background-final-euco-brief-factsheet-overview.pdf.
10. ***, Foreign Affairs Council, EU, 14-15/11/2016, *EU Global Strategy: Implementation Plan on Security and Defence*, https://www.consilium.europa.eu/en/infographics/eu-global-strategy/.
11. ***, Foreign Affairs Council, *Security and Defence Implementation Plan*, EU, 14-15/11/2016, https://www.consilium.europa.eu/en/meetings/fac/2016/11/14-15/.
12. ***, *Standard Eurobarometer 89*, spring, 2018, file:///C:/Users/Asus/AppData/Local/Packages/Microsoft.

MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/eb_89_first_en%20(1).pdf.
13. ***, *Consolidated Version of the European Union Treaty,* in the *European Union Official Journal*, C 83/27, 30.3.2010.
14. C.J.Bickerton, B. Irondelle and A. Menon, *Security Co-operation beyond the Nation-State: The EU's Common Security and Defence Policy*, in *Journal of Common Market Studies*, no. 49(1), 2011.
15. Anna Brosius, Erika J. van Elsas, Claes H. de Vrees, *Trust in the European Union: Effects of the Information Environment*, in the *European Journal of Communication*, 2019, vol. 34(1).
16. Barry Buzan, *Popoarele, statele şi teama*, Editura Cartier, Chişinău, 2000.
17. Pierre Haroche, *Macron's "European Army": Why Is Everyone Talking about It,* in *Euobserver*, Paris, 14 November 2018, https://euobserver.com/opinion/143372.
18. Geoffrey Garrett, George Tsebelis, *An Institutional Critique of Intergovernmentalism*, in *International Organization*, vol. 50, no. 2, spring, 1996.
19. Adrian Ivan, *Guvernanță şi teorii ale integrării în Uniunea Europeană*, course book, Centrul de Studii Europene, Universitatea *"Alexandru Ioan Cuza"*, Iaşi, 2015.
20. Hans J. Morgenthau, *Politica între națiuni. Lupta pentru putere şi lupta pentru pace*, Editura Polirom, Iaşi, 2007.

INTELLIGENCE SUPPORT – AN ESSENTIAL CONDITION FOR SUCCESS IN COUNTERING HYBRID THREATS

Major Ciprian EFIMOV
Graduate student, "Carol I" National Defence University

Today's operational environment is characterised by sophisticated threats posed by various state and non-state actors operating under the threshold of war. Intelligence is a key warfighting function which ensures the coherence of any military action. The author points out the importance of intelligence, which is crucial to every decision-maker, as timely and accurate intelligence makes the difference between success and failure.

In the current security environment, full of numerous and various hybrid threats, intelligence services, which represent the intelligence community of a state or even a political-military alliance, must not only develop intelligence products, but also provide operational solutions, capable of meeting the security issue.

Keywords: intelligence, hybrid threats, theatre of operations, cyber defence, uncertainty.

Introduction

Information is one of the fundamental concepts of the contemporary society. According to the dictionary, the term means "*the communication or reception of knowledge or intelligence; knowledge obtained from investigation, study, or instruction; news, facts, data*"[1]. Extensively, we can say that the information is a communication or news that makes one acknowledge the state and circumstances of various political, military, economic, social, cultural, scientific, and technical processes and phenomena. From the definition, it follows that the planning of every human activity requires accurate and as complete as possible information in order to mitigate the level of uncertainty, and pave the way to achieving the objectives.

The planning of every human activity requires accurate and as complete as possible information in order to mitigate the level of uncertainty, and pave the way to achieving the objectives.

The *hybrid threat* term is a metaphor that brings forward the complexities and dilemmas linked to the ever-changing global security environment. Often, the term is used in the sense of *hybrid warfare*, to underline the interconnected nature of the challenges (ethnic conflicts, terrorism, migration, weak institutions), the multitude of actors involved (regular forces, irregular forces and criminal organisations), and the diversity of the conventional and unconventional means used (military, diplomatic, technologic, informational, etc.). Taking into account the different levels of the threats and the intentions of the actors involved, there is a distinction between the *hybrid threat*, *hybrid conflict*, and *hybrid warfare*[2].

According to the *National Defence Strategy Guide – 2015-2019 (Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019)*, the hybrid threat is defined as *"the threat posed by a state or non-state adversary (individuals, groups), which makes use*

[1] ***, *Merriam Webster Dictionary*, available at https://www.merriam-webster.com/dictionary/information, retrieved on 28 July 2019.

[2] See http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf, retrieved on 6 June 2019.

ROMANIAN MILITARY THINKING

of conventional and unconventional methods and means (political, military, diplomatic, economic, cyber, informational etc.) in a fused and adaptive manner to achieve their objectives"[3].

From the Chinese military theoreticians' perspective – Qiao Liang and Wang Xiangsui, the form of contemporary wars is described as unrestricted warfare. We must admit the fact that the new principles of war do not automatically involve "*using armed force to compel the enemy to submit to one's will",* but rather are *"using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests"*[3].

Nowadays, military operations are employed in a fluid and multidimensional battlespace, characterised by asymmetry, ambiguity, combat actions in five domains (air, land, sea, space, informational), and use of the legal system as a weapon in pursuing strategic objectives, carried simultaneously at every level of military art by state entities, as well as by non-state entities.

Nowadays, military operations are employed in a fluid and multidimensional battlespace, characterised by asymmetry, ambiguity, combat actions in five domains (air, land, sea, space, informational), and use of the legal system as a weapon in pursuing strategic objectives, carried simultaneously at every level of military art by state entities, as well as by non-state entities.

In the hybrid environment, the aggressor may combine deterrence actions (execution of military trainings and exercises according to a scenario which is linked to the targeted state) with actions of the criminal organisations, with information operations (especially through cyber attacks, manipulation of media and population, and using its protest potential to pursuit one's interests), and as the last resort, when its goals were not fulfilled by non-lethal means, the aggressor may engage in combat-specific operations through proxy forces, or, as an extreme solution, open military intervention.

The Importance of Intelligence in the Process of Countering the Hybrid Threats

According to Russian author Alexandr Bartosh, the non-linear character of today conflicts leads to the conclusion that the development of strategies to counter the hybrid threats is of extreme importance. Yet, the success of such an endeavour is conditioned by the multidimensional response, based on timely adaptation of the offensive

[3] ***, *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019,* Bucureşti, 2015, p. 8.

romania2019.eu

and defensive strategies, according to one's own conditions and objectives. Designing such strategies must take into consideration the fact that the presence of a wide range of actors, the development of the events set for fulfilling the planned stepts are not necessarily convergent to what has been intended, but, sometimes, in a totally different, and in many cases, unexpected direction. The existence of such bifurcation points, together with the non-linear character of the hybrid warfare, determines the development of multiple versions, which in concert with the progressive uncertainties to which the subject of the hybrid aggression is exposed, determines the parties involved to make forced, unpredicted choices. From this bifurcation points, the evolution of the political-economic situation may take new meanings, which could lead to regress, inflicting significant damages/losses on the initiator of the hybrid aggression[4].

The early warnings released as a result of the analysis of the information provided by the technical and human sensors are essential for decision-making for designing contingency plans, initiating the planning process for the possible actions to counter the hybrid threats, or adopting concrete measures to eliminate/mitigate the vulnerabilities against hybrid aggression. Such activities help in avoiding the surprise.

The early warnings released as a result of the analysis of the information provided by the technical and human sensors are essential for decision-making for designing contingency plans, initiating the planning process for the possible actions to counter the hybrid threats, or adopting concrete measures to eliminate/mitigate the vulnerabilities against hybrid aggression. Such activities help in avoiding the surprise.

The elevated levels of the complexity and uncertainty of the hybrid confrontational environment require an increasing allocation of resources (financial, materiel, technical and human resources) in order to cover the demands for intelligence necessary to meet political and military decision-makers' needs. The planning, preparation and execution of a military operation against an adversary that uses hybrid tactics, techniques and procedures (TTPs) require detailed and appropriate intelligence about the situation inside the confrontational area, related to the main actors present in the area of interest and their intentions in time and space, evaluation of the hazards, risk, threats, and resources available, able to influence the military actions[5].

[4] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare,* PLA Literature and Arts Publishing House, Beijing, 1999, pp. 6-7, available at https://www.c4i.org/unrestricted.pdf, retrieved on 15 June 2019.

[5] Alexandr Alexandrovici Bartosh, *России не избежать гибридных войн*, Nauchno-Isledovatelnyi Tsentr Problem Natsyonalnyi Bezopastnosti, 9 March 2018 available at http://nic-pnb.ru/vojny-konflikty-voennoe-stroitelstvo/rossii-ne-izbezhat-gibridnyh-vojn/, retrieved on 22 March 2019.

Providing military intelligence during the mission planning, preparation and execution is a force multiplying factor, which gives strength to mission command and ensures force protection. The intelligence cycle, respectively: direction, collection, processing, and dissemination of intelligence[6] related to the hybrid operational environment is a continuous process, directly connected to the battle rhythm.

According to NATO Doctrine, intelligence is one of the fighting functions, together with manoeuvre, fires, command and control, information operation, sustainment, force protection and civil-military cooperation (CIMIC), both at operational components and joint force command levels[7].

According to NATO Doctrine, intelligence is one of the fighting functions, together with manoeuvre, fires, command and control, information operation, sustainment, force protection and civil-military cooperation (CIMIC), both at operational components and joint force command levels.

From the structural perspective, intelligence is an integrant part of the C5I2SR system (Command, Control, Communications, Computers, Cooperation, Intelligence, Interoperability, Surveillance and Reconnaissance). The intelligence sub-system reflects the totality of the procedures, means, personnel, and techniques that meet the intelligence requirements of commanders at every echelon[8].

In order to ensure unit's intelligence support, the collection activities require the use of all forces and means at the commander's disposal at tactical level. Such forces and means include[9]:

- Units at the contact with the enemy;
- Specialised units from combat and support units;
- Reconnaissance patrols;
- Liaison officers assigned to other units;
- Air reconnaissance;
- Maritime reconnaissance, in the river and shore areas.

[6] Alexandru Herciu, *Evaluarea mediului operațional hibrid din perspectiva lecțiilor învățate*, Editura Universității Naționale de Apărare "Carol I", București, 2016, p. 137.

[7] Ovidiu Frățilă, *Prezentarea datelor și informațiilor factorilor de decizie în activitatea de informații militare,* publicat în *Capabilități ale serviciilor moderne de informații militare,* coordonator Sergiu T. Medar, Centrul Tehnic-Editorial al Armatei, București, 2007, p. 312.

[8] ***, *AJP-3(C)*, *Allied Joint Doctrine for the Conduct of Operations*, 2019, p. 1-21, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf, retrieved on 29 July 2019.

[9] Niculai-Tudorel Lehaci, *Tendințe în evoluția sistemului de comandă și control la nivel operativ*, Editura Universității Naționale de Apărare "Carol I", București, 2015, p. 79.

Such activities are specific to the conflict time and are narrowed to the collection capabilities of the tactical units, but the adversary who applies hybrid TTPs is taking action since the peacetime, operating in the grey zone where peace and war are blurred.

In order to have a clear picture of the hybrid operational environment specific to the area of intelligence interest, the tactical units, whether they take action on national territory, or on a host-country territory, as part of a multinational force, will make use of its intelligence/reconnaissance capabilities to cover its intelligence needs as much as possible. Although the tactical units have their own ISR (Intelligence, Surveillance, Reconnaissance) assets, in order to ensure an efficient intelligence support of the commander during the decision-making process, the intelligence support from the higher echelon at operational level, and sometimes, even from the strategic one is essential for understanding the political and social context.

In order to have a clear picture of the hybrid operational environment specific to the area of intelligence interest, the tactical units, whether they take action on national territory, or on a host-country territory, as part of a multinational force, will make use of its intelligence/reconnaissance capabilities to cover its intelligence needs as much as possible.

Interinstitutional Cooperation

Additional to its responsibilities within the Ministry of Defence, the General Directorate for Defence Intelligence contributes to the processes of the National Intelligence Community (NIC). The NIC represents the functional network of the public authorities, parts of the national security system, based on unity of scope, objective and strategy, secured through the intelligence provided by the Romanian Intelligence Service, Foreign Intelligence Service, General Directorate for Defence Intelligence, and General Directorate for Intelligence and Internal Security[10].

By going through the intelligence cycle, the NIC provides, among other intelligence products, a very good coordination of the collection effort, avoidance of unnecessary overlapping, integrated analysis, as well as intelligence support of the state departments with operational responsibilities during the state of emergency, respectively to the Ministry of Internal Affairs, or during the state of siege, respectively the Ministry of Defence[11]. The interinstitutional cooperation is the key

[10] See http://www.administratie.ro/articol.php?id=4921, retrieved on 14 June 2019.

[11] ***, *Legea 453/2004 pentru aprobarea Ordonanței de Urgență a Guvernului nr. 1/1999 privind regimul stării de asediu și regimul stării de urgență*, Art. 2 and 3.

ROMANIAN MILITARY THINKING

effort for every state in the questions related to issuing a timely early warning, initialising the revision of standing plans, and enforcing the preventive measures necessary for successfully countering the hybrid threats during peacetime, and by extension paving the way to success during crisis or war time.

The success against an adversary that applies hybrid TTPs is conditioned by[12]:

- Implementation of a command and control system capable of interinstitutional planning and coordinated implementation of measures, and of integrated execution of national defence activities;
- The capacity of the military command and control system to generate and sustain a relative superiority of the intelligence and decision cycles;
- The capacity to completely integrate the intelligence obtained through own assets;
- The assurance of early warning services, through a centralised dissemination of messages, or alarming of the personnel related to operational situation in their stations;
- Possession of the capabilities able to guarantee cyber defence;
- The performance of the processes for information assurance of the communication and informatics systems;
- The level of the readiness, flexibility, modularity, mobility, deployable forces, sustainability, and interoperability of the armed forces.

In order to accomplish their missions at strategic level, the military intelligence structures must possess collection, integration and processing of intelligence, and dissemination capabilities able to prevent the strategic surprise, by permanently keeping national decision-making authorities, allies and partners informed.

Missions of the Intelligence Structures

In order to accomplish their missions at strategic level, the military intelligence structures must possess collection, integration and processing of intelligence, and dissemination capabilities able to prevent the strategic surprise, by permanently keeping national decision-making authorities, allies and partners informed.

[12] ***, *Carta Albă a Apărării, Ministerul Apărării Naționale*, București, 2017, pp. 37-38.

romania2019.eu

The performance of a strategic surprise prevention system is conditioned especially by[13]:

- Technological level and the capacity of the intelligence capabilities to provide actionable, timely and viable intelligence;
- The flexibility, modularity and resilience of the defence intelligence system, and its interoperability with similar NATO and EU systems;
- The required level of the capacity to collect, verify, process and exploit the information related to the internal and external, military and non-military risks and threats;
- The required level of the capacity to identify the vulnerabilities and risks, to prevent and counter the threats specific to cyber space;
- The technological level of cryptographic systems designed for protection of the classified information and its interoperability with the similar NATO and EU systems.

According to intelligence specialists, the missions that must be covered by an efficient *ISR system* at all levels of command, from the political-strategic one to the operational and tactical ones, are[14]:

- Early warning – implies issuance of the early warning in such a way that the surprise is avoided, by anticipating and mitigating the risk generated by the adversaries' actions; it allows for military decision-makers to organise in due time their forces, to adjust the structure of the units according to the nature of the identified threat, in order to efficiently counter the unpredictable situations, to decide whether or not the forces readiness must be increased or if it is necessary to deploy its troops in a designated theatre of operations. Within the operational framework, the intelligence structures must identify those threats, real or possible, that can change the nature of the operation, as: the possible use of weapons of mass destruction, violation of international treaties and agreements,

[13] *Ibid*, pp. 39-40.

[14] Ionel Irimia, Răzvan Mofleanu, *Sistemele de informații, supraveghere și cercetare – factor de bază al capacității de anticipare și acțiune pro-activă a structurilor de forțe,* Conferința Doctrinară a Forțelor Terestre, 28-29 October 2009, available at http://www.revista.forter.ro/cd_2009/03-sub3/031.htm, retrieved on 20 June 2019.

unexpected deployment of troops in the expected area of operations, unexpected change of adversary's intentions, and changing attitude of the local population towards some actions;

- Intelligence support for operations planning process. Operations planning starts with a thorough analysis of the crisis/situation and its triggering causes, of different actors and systems present in the engaging area, from the perspective of their motivation, strengths, vulnerabilities, interactions, and interdependencies;

Provision of intelligence about the enemy and environment necessary to visualise/understand the common operational picture and to contribute to understanding the situational awareness;

- Delivery of intelligence about targets – contributes to target prioritisation based on their importance;
- Information operations (IO) support. Currently, IOs are carried both during modelling operations and during decisive ones. In some cases, IO are enough to reach the ends of the operation (the manipulation of the population's protest potential to change a government hostile to the interests of the IO initiator);
- Provision of the intelligence needed for the assessment of the situation and the risks;
- Force protection – involves the identification, localising, and pursuit of enemy's capabilities to hit and affect friendly forces. In this respect, the military intelligence structures accomplish the following tasks: identify and counter the adversary's collection capabilities, assess the friendly forces' vulnerabilities and the adversary's capacity to identify and exploit them, identify the enemy's perception on friendly forces' main capabilities and the way that the enemy intends to approach them, identify the essential countermeasures to deny enemy's access to friendly forces' critical capabilities, and perform risk and threat assessment.

Force protection – involves the identification, localising, and pursuit of enemy's capabilities to hit and affect friendly forces. In this respect, the military intelligence structures accomplish the following tasks: identify and counter the adversary's collection capabilities, assess the friendly forces' vulnerabilities and the adversary's capacity to identify and exploit them, identify the enemy's perception on friendly forces' main capabilities and the way that the enemy intends to approach them, identify the essential countermeasures to deny enemy's access to friendly forces' critical capabilities, and perform risk and threat assessment.

In the context of today's conflicts, actions carried out at tactical level (some special forces missions, as for instance the capturing of Osama bin Laden) may have a strategic impact, just as some intelligence regarding to strategic targets must be shared with commanders

at tactical level in order to accomplish the assigned missions. In this respect, intelligence collection required to identify the main targets falls under the military intelligence structures' responsibility at every level of military art. Moreover, a precise assessment of overall inflicted damages may lead from exploit of success (at tactical-operational level) to cessation of hostilities and bringing the adversary to the negotiation table(at political-strategic level), which leads to the conclusion that the accurate evaluation of the inflicted damage at all levels, including the strategic one, should be one of the missions of the strategic military intelligence structure.

In addition, Sergiu Medar, PhD, identifies as strategic intelligence structures' missions, among issuance of the early warning, intelligence preparation of the battlefield, estimation of the fighting capacity of the enemy, and force protection, *the identification of the main targets to be destroyed/neutralised, and the evaluation of the damages inflicted on the enemy*[15].

Within nowadays security environment, packed with hybrid threats posed by state and non-state actors, the intelligence services, part of the intelligence community of a state or of a political-military alliance, are facing the stances when they must not only design intelligence products,*"but also provide operational solutions to meet some societal and security related issues"*[16].

Within nowadays security environment, packed with hybrid threats posed by state and non-state actors, the intelligence services, part of the intelligence community of a state or of a political-military alliance, are facing the stances when they must not only design intelligence products, "but also provide operational solutions to meet some societal and security related issues".

The intelligence collection to ensure the national security is achieved by priorities and in the limits of the available resources to identify and prevent the harmful effects of: espionage; sabotage; economic and political undermining of the state, democracy, constitutional order; subversive actions; terrorism; organised crime; endangerment of informatics infrastructure; aggressions against critical systems (transportation, energy, communications, vital systems for life etc.); and aggressions against command and control system of decision-making acts in the security realm. Having covered

[15] Sergiu T. Medar, *Relația decident militar-lider al structurilor de informații militare,* pp. 23-25, published in *Capabilități ale serviciilor moderne de informații militare,* coord. Sergiu T. Medar, Centrul Tehnic-Editorial al Armatei, București, 2007.

[16] Petre-Gabriel Burdușel, *Locul şi rolul Intelligence în combaterea amenințărilor de tip hibrid*, UNAp, București, 2018, p.53.

ROMANIAN MILITARY THINKING

this domains, the intelligence community will be able to identify in due time the symptoms of the hybrid threats[17].

The hybrid threats seek to produce effects on national security, and thus influence the constitutional order by violating the state's sovereignty and independence, unity and indivisibility. In the situation when a threat to national security is identified, especially a hybrid one, the intelligence products are fundamental to decreeing the state of emergency, siege, or by case, mobilisation, or war, including the activation of response measures at inter-institutional level by deploying troops on the ground, be it for countering a hybrid threat within the national borders, or abroad, as part of a multinational force.

In the situation when a threat to national security is identified, especially a hybrid one, the intelligence products are fundamental to decreeing the state of emergency, siege, or by case, mobilisation, or war, including the activation of response measures at inter-institutional level by deploying troops on the ground, be it for countering a hybrid threat within the national borders, or abroad, as part of a multinational force.

Even if the intelligence is considered of extreme importance for a successful countering of the hybrid threats, especially when it comes to the early warning about a potential threat, there is a risk linked to the ego and convictions of some decision-makers to omit, more or less intentionally, some reports and analysis coming from intelligence services, and thus, to miss the opportunity to inhibit in the early stage the hybrid threats posed by the adversaries. Furthermore, the subjectivity of some intelligence analysts eager to be in line with the decision-maker's vision may lead to adopting some decisions that do not reflect the reality on the field, therefore affecting the image of the institution, or even of the state, creating in this way an easily exploitable vulnerability by the state and non-state actors adopting hybrid TTPs.

A good example related to the importance of intelligence in countering the hybrid threat is the annexation of Crimea by Russian Federation. Kremlin's intention was anticipated neither by western intelligence services, nor by the Ukrainian services so that they could be able to adopt some counter-measures, and implicitly to ask for international support to prevent the situation. The failure of the Ukrainian intelligence community, and not only, to identify the threat and issue an early warning in this respect has led to strategic surprise in the cases of both Kiev and the West. The situation created did not make it possible for coherent mobilisation to take place in order

[17] *Ibid*, p. 59.

to repel the hybrid threat. Furthermore, it gave Moscow enough time to pursue and reach its strategic objectives unhindered.

romania2019.eu

Conclusions

Consequently to the accelerated progress of information technology and easy access of masses to information, in the confrontational environment of the past three decades, the IO have been omnipresent, as a must for preparing and conducting operations, demonstrating its efficiency. In the US Navy Strategy for Achieving Information Dominance, the US Navy Chief of Operations, Jonathan Greenert, stated that in modern war *"control of information – much of it through the electromagnetic spectrum – is already growing more important than the control of territory in modern warfare"*[18]. In today's context, information is being deployed as a weapon, cyberspace as a warfighting domain, and the network and electromagnetic spectrum comprise the battlespace[19].

The importance of information leads to the idea that military art should be adjusted to the contemporary realities by including *the information domination principle* among its principles. To apply/follow this new principle, it is necessary that the intelligence structures are equipped with cutting-edge technologies in order to assure intelligence collection from all sources, as well as to ensure quality training for the technical operators, and for human resource assigned to collect and process the intelligence gathered through collection capabilities (HUMINT, SIGINT, IMINT etc). Additionally, the assurance of information dominance requires that protection/defensive programmes and technologies are implemented against cyberattacks, electronic warfare, and the population is trained to better defend itself against manipulation, psychological influencing, intelligence actions, or familiarisation/training of population related to the distinction between fake news and the real ones. In this equation, the structures capable to conduct IO should be comprised, which should assess,

The importance of information leads to the idea that military art should be adjusted to the contemporary realities by including the information domination principle among its principles. To apply/follow this new principle, it is necessary that the intelligence structures are equipped with cutting-edge technologies in order to assure intelligence collection from all sources, as well as to ensure quality training for the technical operators, and for human resource assigned to collect and process the intelligence gathered through collection capabilities (HUMINT, SIGINT, IMINT etc).

[18] ***, *Navy Strategy for Achieving Information Dominance 2013-2017,* p. 5, available at https://www.public.navy.mil/fcc-c10f/Strategies/Navy_Strategy_for_Achieving_Information_Dominance.pdf, retrieved on 08 March 2019.

[19] *Ibid*, p. 3.

monitor, and report population's level of resilience to a potential hybrid aggression.

Having secured information dominance, or at least a level that is equal with our main state/alliance adversaries, we can call for an efficient and effective intelligence support, which constitutes the essential factor for successfully countering hybrid threats.

BIBLIOGRAPHY

1. ***, *AJP-3(C), Allied Joint Doctrine for the Conduct of Operations*, NATO, 2019.
2. ***, *Carta Albă a Apărării*, Ministerul Apărării Naționale, Bucureşti, 2017.
3. ***, *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019, Administrația Prezidențială*, Bucureşti, 2015.
4. Alexandr Alexandrovici Bartosh, *России не избежать гибридных войн (Russia Can't Avoid Hybrid Wars),* Nauchno-Isledovatelnyi Tsentr Problem Natsyonalnyi Bezopastnosti, 9 March 2018.
5. Petre-Gabriel Burduşel, *Locul şi rolul Intelligence în combaterea amenințărilor de tip hibrid*, Universitatea Națională de Apărare „Carol I", București, 2018.
6. Ovidiu Frățilă, *Prezentarea datelor şi informațiilor factorilor de decizie în activitatea de informații militare*, published in *Capabilități ale serviciilor moderne de informații militare*, coordonator Sergiu T. Medar, Centrul Tehnic-Editorial al Armatei, Bucureşti, 2007.
7. Alexandru Herciu, *Evaluarea mediului operațional hibrid din perspectiva lecțiilor învățate*, Editura Universității Naționale de Apărare „Carol I", București, 2016.
8. Marian Iordache, *Particularități privind sprijinul cu informații al structurilor convenționale tactice de nivel divizie care desfăşoară operații de contrainsurgență, în contextul războiului hibrid*, Universitatea Națională de Apărare „Carol I", București, 2018.
9. Ionel Irimia şi Răzvan Mofleanu, *Sistemele de informații, supraveghere şi cercetare – factor de bază al capacității de anticipare şi acțiune proactivă a structurilor de forțe*, Conferința doctrinară a Forțelor Terestre, 28-29 October 2009.
10. Niculai-Tudorel Lehaci, *Tendințe în evoluția sistemului de comandă şi control la nivel operativ*, Editura Universității Naționale de Apărare „Carol I", București, 2015.
11. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, 1999.
12. Sergiu T. Medar, *Capabilități ale serviciilor moderne de informații militare*, Centrul Tehnic-Editorial al Armatei, Bucureşti, 2007.

WEBOGRAPHY

1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623172/doctrine_nato_conduct_op_ajp_3.pdf
2. https://dexonline.ro/definitie/informa%C8%9Bie
3. http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf
4. https://www.public.navy.mil/fcc-c10f/Strategies/Navy_Strategy_for_Achieving_Information_Dominance.pdf.

ROMANIAN MILITARY THINKING

romania2019.eu

THE EAST-WEST CONFRONTATION AND THE NEW COLD WAR

Professor Mihail ORZEAȚĂ, PhD
"Apollonia"University, Iaşi

The present article is meant to remind all the readers that international security is in the process of deteriorating as many states would rather resort to confrontation to resolve the existing issues between them than to negotiation or cooperation[1].

It is not the first time when the interstate rivalry "generates extraordinary security concerns anticipating armed conflict"[2]. The tense relations between the West (NATO and EU) and Russia have a negative influence over international relations as well as over regional and global security. The most important situation is the relation of "an eye for an eye"[3] type between different states, a pretty common situation occurred during the Cold War as well as today.

Keywords: East-West relations, global security, international relations, authoritarianism, interstate rivalry.

1. Introduction

The map of the world is red, considering the ongoing violent clashes that make thousands of victims daily, destroying critical infrastructure that plays a vital role in the lives of the citizens in the areas of operation, forcing them to leave their homes to save, thus becoming refugees, emigrants, asylum seekers or even stateless people.

The accession, in an increasing number of states, to decision-making positions of some leaders having authoritarian tendencies[4] or of extremist parties[5] represents one of the most important causes for the use of force in the relations between states or in those between the communities within states.

Frozen conflicts simmer[6] under the *"thin crust"* of some treaties and agreements kept in force with the help of peacekeeping troops.

International security at regional and global level is negatively influenced by the tense relations between the West (NATO plus EU) and Russia, characterised by an increasing number of political theorists, security experts and journalists as the *"New Cold War"*[7].

International security at regional and global level is negatively influenced by the tense relations between the West (NATO plus EU) and Russia, characterised by an increasing number of political theorists, security experts and journalists as the "New Cold War".

International governmental organisations having responsibilities in the field of ensuring security at global level (the UN)[8] as well as at regional level (Organisation for Security and Cooperation in Europe – OSCE, Organisation of American States – OAS, Organisation of African Unity – OUA, Arab League – AL)[9] seem to be less and less relevant as they have not managed to stop the evident tendency towards violence

---

1 Henry Kissinger, *Diplomația*, Editura BIC ALL, Bucureşti, 2007, p. 16.

2 Johann Park and Chungshik Moon, *Interstate Rivalry and Interstate Trade*, in *The Chinese Journal of International Politics*, 2018, vol. 11, nr. 3, p. 284, https://1b596b46-a-62cb3a1a-s-sites.googlegroups.com/site/parkjoha/rivalry%20and%20trade%20published.pdf?, retrieved on 10.05.2019.

3 Teodor Danalache, *Ochi pentru ochi, dinte pentru dinte!*, Crestin Ortodox.ro, 30 July 2009, https://www.crestinortodox.ro/religiile-lumii/iudaism/legea-talionului-125032.html, retrieved on 16.04.2019.

English version by **Diana Cristiana LUPU**.

4 Aamna Mohdin, *Populist, Authoritarian Leaders Are Still on the Rise across Europe*, Quartz, 12 July 2017, https://qz.com/1027518/populist-authoritarian-leaders-are-still-on-the-rise-across-europe/, retrieved on 14.05.2019.

5 Goran Buldioski, *EU Must Confront Poland and Hungary*, EUObserver, Budapest, 21 November 2017, https://euobserver.com/opinion/139942, retrieved on16.05.2019.

6 Madeleine Albright, *Doamna secretar de stat. Memorii*, Editura Rao, Bucureşti, 2008, p. 537.

7 Edward Lucas, *The New Cold War: Putin's Russia and the Threat to the West*, 17 March 2009.

8 Madeleine Albright, *Who Broke the U.N.*?, in *Foreign Policy*, 13.08.2012, http://foreignpolicy.com/2012/08/13/who-broke-the-u-n/, retrieved on 19.12.2014.

9 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 11.05.2019.

ROMANIAN MILITARY THINKING

in international relations, in general, and in the relations between the West and the Russian Federation, in particular.

2. Summary of the Cold War History

All historians, political theorists and experts in international security credit Winston Churchill as the author of the *"Iron Curtain"*[10] phrase, which later became synonymous with the Cold War[11]. Churchill firstly used the *"Iron Curtain"* phrase publicly in a speech delivered in the House of Commons of the UK Parliament on 16 August 1945, protesting against the decision of the Soviet Union to contain the UK Embassy in Bucharest within an iron fence[12]. History retained the first public use of the phrase *"Iron Curtain"* as being the *"Sinews of Peace"* speech delivered by W. Churchill at Westminster College, Fulton, Missouri, the USA, on 5 March 1946. The phrase was also mentioned by the President of the USA, Harry Truman, born in that state, in front of a larger audience than the population of Fulton. The former Prime Minister of the UK had the idea of the *"Iron Curtain"* in 1945 and he used it for the first time on 12 May 1945[13], in a telegram addressed to President Truman, expressing his concern for the future of Europe and the states occupied by the Soviet Union.

The animosities between the former allies in the Second World War – the USA and the UK, on the one hand, and the USSR, on the other hand – arose even during the armed confrontations with the Axis states because of certain geopolitical and geostrategic interests, namely different views on the new post-war world order and attitudes towards the defeated states.

The animosities between the former allies in the Second World War – the USA and the UK, on the one hand, and the USSR, on the other hand – arose even during the armed confrontations with the Axis states because of certain geopolitical and geostrategic interests, namely different views on the new post-war world order and attitudes towards the defeated states.

The USA and the UK wanted the establishment of democracy in the Axis states and their satellites, and the Soviet Union, through Stalin's voice, argued that each victorious state should impose its political regime in the states it occupied. The Westerners also wanted to establish an international criminal court to investigate war crimes[14], while Stalin advanced the proposal to exterminate 50,000 high-ranking military personnel in Germany, so that it could no longer rise to pre-war status for a long period of time and trigger another world war[15].

Stalin's exaggerated demands were rejected by the UK Prime Minister, Churchill, using acid words, and the US President, Franklin Delano Roosevelt, proved more conciliatory, mediating between the two in order to keep the Entente united[16].

Following Roosevelt's death, on 12 April 1945, Harry Truman became the President of the USA. As he did not agree with the Russians[17], the relations with Stalin changed. Although Truman knew the request made by his predecessor during the *"Big Three"* Conference in Tehran (November-December 1943), resumed in Yalta (February 1945) and accepted by Stalin, for the Soviet Union to participate in the Pacific War against Japan, after Nazi Germany was defeated, the new US President trenchantly stated that the USSR involvement in the Pacific War was *"neither necessary nor desirable"*[18]. Not considering the position expressed by the USA, the Soviet troops launched the ground offensive against Japan, despite the existing Russian-Japanese nonaggression treaty, respected by the Japanese throughout the war in Europe, occupying Manchuria, Outer Mongolia, Sakhalin region and part of the Kurile Islands, up to late August 1945[19].

Following Roosevelt's death, on 12 April 1945, Harry Truman became the President of the USA. As he did not agree with the Russians, the relations with Stalin changed. Although Truman knew the request made by his predecessor during the "Big Three" Conference in Tehran (November-December 1943), resumed in Yalta (February 1945) and accepted by Stalin, for the Soviet Union to participate in the Pacific War against Japan, after Nazi Germany was defeated, the new US President trenchantly stated that the USSR involvement in the Pacific War was "neither necessary nor desirable".

Called also the *"war that was not waged"* and the *"war for which each side was preparing but did not want it to break out"*[20], the Cold War initially had the USA and the USSR as protagonists. After the establishment of the two political-military blocs – NATO on 4 April 1949 and the Warsaw Pact on 14 May 1955 – the confrontation was conducted between the two alliances.

[10] The Sinews of Peace *("Iron Curtain Speech")*, 5 March 1946, Westminster College, Fulton, Missouri, International Churchill Society, https://winstonchurchill.org/resources/speeches/1946-1963-elder-statesman/the-sinews-of-peace/, retrieved on 12.05.2019.

[11] *Winston Churchill's Iron Curtain: from Russia with Labour*, History Answers, https://www.historyanswers.co.uk/people-politics/did-this-painting-foresee-the-rise-of-adolf-hitler/, retrieved on 13.05.2019.

[12] Thomas Parish, *Enciclopedia Războiului Rece*, Editura Univers Enciclopedic, București, 2002, p. 83.

[13] Scott Michael Rank (editor), *Winston Churchill's Iron Curtain Speech: Predicting the Cold War*, History on the Net, https://www.historyonthenet.com/winston-churchills-iron-curtain-speech-predicting-the-cold-war, retrieved on 14.05.2019.

[14] Alessandra Minerbi, *Istoria ilustrată a nazismului*, Editura Rao, București, 2006, p. 179.

[15] Michael D. Hull, *The Big Three in Tehran: The Meeting that Shaped WWII*, Warfare History Network, 12 December 2018, https://warfarehistorynetwork.com/daily/wwii/the-big-three-in-tehran-the-meeting-that-shaped-wwii/, retrieved on 14.05.2019.

[16] *Ibidem.*

[17] Arnold A. Offner, *President Truman and the Origins of the Cold War*, BBC http://www.bbc.co.uk/history/worldwars/wwtwo/truman_01.shtml, last updated on 17.02.2011, retrieved on 10.05.2019.

[18] H.P. Willmott, *The Second World War in the Far East*, Cassell & Co, Wellington House, London, 1999, p. 205.

[19] *Ibidem*, pp. 206-207.

[20] Laurence Freedman, *The Cold War. A Military History*, Cassell & Co, London, 2001, pp. 18, 204-205.

Considering its development, the Cold War blurred the distinction between peace and armed fight[21], as it was not a sum of victories and defeats but more a peace based on the balance of power[22], being achieved following a series of crises, having different scope and intensity. Among them, the most important one was considered the Cuban Missile Crisis (1962)[23], which could result in a nuclear war between the USA and the USSR.

Each party in the confrontation intended to have global hegemony[24] and to impose own ideology: the USA promoted liberal democracy, while the USSR supported communism. Therefore, they employed the following methods:

- direct confrontations in the political, diplomatic and economic-financial fields;
- proxy armed confrontations[25] (Korea: 1950-1953; Vietnam: 1964-1972; Afghanistan: 1979-1989; Arab-Israeli wars);
- espionage, manipulation, propaganda, disinformation and psychological operations to influence the international community and the adversary population;
- interference in the adversary sphere of influence;
- boycott of sports events (the Western states boycotted the Olympic Games in Moscow, in 1980, to protest against the invasion of Afghanistan by the Soviets, and, in retaliation, the USSR and the socialist states, except for Romania, boycotted the Olympic Games in Los Angeles, in 1984[26]), as well as of international cultural and political events held in states belonging to the adversary bloc;
- arms race[27], space race[28] etc.

[21] Simon Trew, Garry Sheffield, editors, *100 Years of Conflict 1900-2000*, Sutton Publishing Limited, Phoenix Mill, UK, 2000, p. 263.
[22] Laurence Freedman, *op. cit.*, pp. 17, 204, 205.
[23] *Cuban Missile Crisis*, John F. Kennedy Presidential Library and Museum, http://www.jfklibrary.org/JFK/JFK-in-History/Cuban-Missile-Crisis.aspx, retrieved on 03.05.2015.
[24] William Pfaff, *The Question of Hegemony*, Foreign Affairs, January-February 2001, https://www.foreignaffairs.com/articles/2001-01-01/question-hegemony, retrieved on 19.12.2014.
[25] Simon Trew, Garry Sheffield, *op. cit.*, p. 261.
[26] Thomas Parish, *op. cit.*, p. 46.
[27] Sam Perlo-Freeman, *Arms race*, Encyclopaedia Britannica, https://www.britannica.com/topic/arms-race, retrieved on 08.05.2019.
[28] John McNeer, *The Space Race in the Context of the Cold War*, History Arch, 20 July 2018, https://historyarch.com/2018/07/20/the-space-race-in-the-context-of-the-cold-war/, retrieved on 08.05.2019.

Being superior in terms of economy and political-diplomatic influence, the USA implemented, following the suggestion of its former ambassador in Moscow, George Keenan[29], the strategy to contain the USSR, which became the *Truman Doctrine*, materialised in a system of alliances (Australia, New Zealand and the United States of America – ANZUS, South East Asia Treaty Organisation – SEATO[30] etc.). To the mentioned treaties and alliances there were added the Baghdad Pact or CENTO, initiated by the United Kingdom (including Turkey, Iraq, Iran and Pakistan). It was aimed at denying the USSR access to the Persian Gulf region, which was rich in oil and natural gas resources, thus supplying the Western states[31]. The alliance system was completed and supported by the establishment of military bases in the countries in the neighbourhood of the Warsaw Pact member states, especially the USSR (Island, the Federal Republic of Germany, Turkey, Greece, Japan, South Korea, the Philippines etc.).

Officially, the end of the Cold War was a consequence of the meeting and agreements between the US President, Ronald Reagan, and the Soviet President, Mikhail Gorbachev, in November 1989, in Malta[32]. Practically, the abolition of the Warsaw Pact, in 1990, and the dissolution of the USSR, in 1991, were two of the most important events that certified the end of the Cold War. Some authors considered those events as sanctioning the victory of liberal democracy against totalitarianism[33], thus opening the path towards the economic warfare[34]. Other authors considered the mentioned victory as *"ambiguous"*[35].

Officially, the end of the Cold War was a consequence of the meeting and agreements between the US President, Ronald Reagan, and the Soviet President, Mikhail Gorbachev, in November 1989, in Malta. Practically, the abolition of the Warsaw Pact, in 1990, and the dissolution of the USSR, in 1991, were two of the most important events that certified the end of the Cold War.

[29] *MILESTONES: 1945-1952, Keenan and Containment, 1947, US Department of State, Office of the Historian*, https://history.state.gov/milestones/1945-1952/kennan, retrieved on 04.01.2015.
[30] Pierre Milza and Serge Berstein, *Istoria secolului XX*, vol. 2, Editura BIC All, Bucureşti, 1998, p. 29.
[31] Ivakos Alkadeff, *A Comparison between Cold War 1 and Cold War 2*, Word Press, 4 November 2015, https://iakal.wordpress.com/2015/11/04/a-comparison-between-cold-war-1-and-cold-war-2/,retrieved on 17.07.2019.
[32] Thomas Parish, *op. cit.*, p. 55.
[33] Francis Fukuyama, *America la răscruce*. *Democrația, puterea şi moştenirea neoconservatoare*, Editura Antet XX Press, Filipeştii de Târg, Prahova, 2006, p. 49.
[34] Fred C. Bergsten, *Japan and the United States in the New World Economy*, published by Theodore Rueter, in *The United States in the World Political Economy*, Mc Graw-Hill, New York, 1994, p. 175.
[35] Ronald Steel, *Temptations of a Superpower*, Harvard University Press, 1995, pp. 6-23.

ROMANIAN MILITARY THINKING

3. Similarities and Differences between the Cold War and the Current Situation in the East-West Confrontation

3.1. Similarities between the East-West Relations during the Cold War Period and the Current Ones

The comparative analysis of the East-West relations during the Cold War period and the current ones reveals a number of similarities[36], materialised in direct or subversive confrontation in the political, diplomatic, economic, financial, information, cultural and military fields[37].

3.1.1. Confrontation Measures Reciprocally Employed by Both Sides

The different interests of the West and of the Russian Federation in the political-diplomatic, economic-financial, information and military fields have resulted in both sides reactions, having different scope and intensity, materialised in:

- political-diplomatic and economic-financial embargo[38], applied in the form of reciprocal sanctions[39] of *"an eye for an eye, a tooth for a tooth"* type[40];
- psychological influence of the international community[41] and of the adversary population employing manipulation[42], propaganda, disinformation and *"declaration warfare"*[43];
- interference in the adverse party domestic policy[44];
- undeclared arms race[45];
- deployment of forces[46] and real military exercises in border areas[47];
- proxy military confrontations[48];
- shows of force.

3.1.2. Confrontation Measures Initiated by the West and Addressed to the Russian Federation

Following Russia's intervention in the war between Georgia and South Ossetia (August 2008), the North Atlantic Council decided, on 19 August 2008, to suspend NATO-Russian Federation meetings until the withdrawal of the Russian troops from Georgia.

Following the annexation of Crimea by Russia, the North Atlantic Council decided to cancel all the actions meant for the cooperation with the Russian Federation, except for the Political Dialogue[49].

On the initiative of Western states, the UN General Assembly condemned Russia, after the annexation of Crimea[50].

The Western states that are G8 members decided to exclude Russia from this international forum[51].

romania2019.eu

Following Russia's intervention in the war between Georgia and South Ossetia (August 2008), the North Atlantic Council decided, on 19 August 2008, to suspend NATO-Russian Federation meetings until the withdrawal of the Russian troops from Georgia. Following the annexation of Crimea by Russia, the North Atlantic Council decided to cancel all the actions meant for the cooperation with the Russian Federation, except for the Political Dialogue. On the initiative of Western states, the UN General Assembly condemned Russia, after the annexation of Crimea.

---

[36] Edward Lucas, *The New Cold War: Putin's Russia and the Threat to the West*, Palgrave McMillan, 2009, New York, USA, the book review is available at http://www.amazon.com/the-new-cold-war-putins/dp/02302614345#reader-0230614345, retrieved on 20.07.2014; see also Yevgeny Shestakov, *Russia and the West: Neither Cold War Nor Warm Peace*, *The Telegraph*, 03.01.2013, http://www.telegraph.co.uk/sponsored/rbth/opinion/9777516/russia-west-cold-war.html, retrieved on 11.08.2014.

[37] Simon Tisdall, *The New Cold War: Are We Going Back to Bad Old Days?*, in *The Guardian*, 19.11.2014, http://www.theguardian.com/world/2014/nov/19/new-cold-war-back-to-bad-old-days-russia-west-putin-ukraine, retrieved on 30.12.2014.

[38] Shiva Shankar Pandian, Kayra Watson, *Tit-for-Tat: Russia Expels 59 Diplomats from 23 Countries in Retaliation*, 31 March 2018, https://www.uscpublicdiplomacy.org/blog/tit-tat-diplomatic-expulsions-and-closures, retrieved on 15.04.2019.

[39] UN Charter, Chapter VIII, http://www.un.org/en/documents/charter/chapter8.shtml, retrieved on 05.05.2019.

[40] Alistar Heath, *Tit-for-Tat Trade War with Russia Will Hurt Many but Achieve Little*, in *The Telegraph*, 7 August 2014, https://www.telegraph.co.uk/finance/economics/11020242/Tit-for-tat-trade-war-with-Russia-will-hurt-many-but-achieve-little.html, retrieved on 15.04.2019.

[41] Shaun Walker, *Dmitry Medvedev Visits Crimea as Russia's Army Begun Border Withdrawal*, in *The Guardian*, 31.03.2014, http://www.theguardian.com/world/2014/mar/31/dmitry-medvedev-crimea-army-border-withdrawal-ukraine, retrieved on 01.04.2014.

[42] Ben Farmer, *I Can Take Kiev in Two Weeks, Vladimir Putin Warns European Leaders*, in *The Telegraph*, 01.09.2014, http://www.telegraph.co.uk/news/worldnews/ukraine/11069070/I-can-take-Kiev-in-two-weeks-Vladimir-Putin-warns-European-leaders.html, retrieved on 02.09.2014.

[43] Olga Krasnyak, *Tit for Tat: Diplomatic Expulsions and Closures*, Center on Public Diplomacy (CPD), 13 September 2017, https://www.uscpublicdiplomacy.org/blog/tit-tat-diplomatic-expulsions-and-closures, retrieved on 15.04.2019.

[44] *Ibidem*.

[45] Jason Lemon, *New Russian Weapons 'Significantly Increase' Military's Potential, Putin Warns Rivals*, Newsweek, 12/18/18, https://www.newsweek.com/russian-weapons-military-potential-putin-warns-1262973, retrieved on 20.12.2018.

[46] Mark Thompson, *Russian Forces Double along Ukraine Border*, Time, 28.03.2014, http://time.com/41490/russia-ukraine-crimea-putin/, retrieved on 14.04.2015.

[47] Michael Birnbaum, *Fearing Russian Expansion Baltic Nations Step up Military Exercises*, in *The Washington Post*, 16.05.2015, http://www.washingtonpost.com/world/europe/fearing-russian-expansion-baltic-nations-step-up-military-exercises/2015/05/15/b5ee51ee-f8c8-11e4-a47c-e56f4db884ed_story.html, retrieved on 01.06.2015.

[48] Tom O'Connor, *U.S. vs. Russia in Syria: These Are Their Top Weapons*, Global Geopolitics, 13 April 2018, Posted with permission from Newsweek, http://globalgeopolitics.net/2018/04/13/u-s-vs-russia-in-syria-these-are-their-top-weapons/, retrieved on 14.04.2019.

[49] Statement by NATO Foreign Ministers, North Atlantic Treaty Organization, 01.04.2014, http://www.nato.int/cps/en/natohq/news_108501.htm, retrieved on 10.05.2015; see also *Relations with Russia, North Atlantic Treaty Organization*, last updated: 04.02.2019, https://www.nato.int/cps/en/natohq/topics_50090.htm, retrieved on 14.05.2019.

[50] Louis Charbonneau, *Russia Threatened Countries ahead of UN Vote on Ukraine, Diplomats Say*, Reuters, 28.03.2014, http://www.huffingtonpost.com/2014/03/28/exclusive-russia-ukraine_n_5052313.html, retrieved on 29.03.2014.

[51] Clemens Bilan, *German MP: Russia's Exclusion from G8 'Wrong from Very Beginning'*, Sputnik News, 05.01.2016, https://sputniknews.com/politics/201601051032705436-germany-g8-russia/, retrieved on 14.05.2019.

Many Western states and Australia threatened Russia with political-diplomatic and economic-financial isolation, through sanctions in these domains[52], threat that was enacted.

To meet the goal of isolating Russia, the US Secretary of State, John Kerry, visited China[53] and India[54], to persuade these countries to rally to the Western initiative.

3.1.3. Confrontation Measures Initiated by the Russian Federation Addressed to the West

The sanctions applied to Russia by the West have prompted Moscow to retaliate and to review the security strategy. The most important measures are the following:

- the nominalisation of NATO as the greatest threat to Russia's security[55];
- the obstruction of certain initiatives in the UN Security Council[56];
- the initiation, in cooperation with BRICS member states (Brazil, Russia, India, China and South Africa), Venezuela and Iran, of some measures so that the dollar will not be the single currency in international trade transactions (the so-called *"de-dollarization"*[57]);
- the establishment of an international development bank to break up the monopoly of the International Monetary Fund (IMF) where the USA has a dominant position; the agreement

[52] Roberta Rampton, *Biden Warns Russia Will Be Isolated If Ukraine Crisis Not Resolved: US Official*, *Reuters*, 3 March 2014, http://news.yahoo.com/biden-warns-russia-isolated-ukraine-crisis-not-resolved-174333462.html, retrieved on 03.01.2015.

[53] Julie Pace and Matthew Lee, *Hoping to Isolate Russia, US Woos China on Ukraine*, in *Associated Press*, 11.03.2014, http://www.irrawaddy.org/asia/hoping-isolate-russia-us-woos-china-ukraine.html, retrieved on 12.08.2014.

[54] Ajay Kamalakaran, *Time for India to Stand by Russia, Russia beyond the Headlines,* 01.08.2014, http://in.rbth.com/blogs/2014/08/01/time_for_india_to_stand_by_russia_37133.html, retrieved on 11.08.2014.

[55] Maria Tsvetkova, *Russia's New Military Doctrine Names NATO as Key Risk*, *Reuters*, 26.12.2014, http://www.reuters.com/article/2014/12/26/us-russia-crisis-military-doctrine-idUSKBN0K40Q120141226, retrieved on 27.12.2014.

[56] UN Security Council action on Crimea referendum blocked, UN News Centre, 15.03.2014, http://www.un.org/apps/news/story.asp?NewsID=47362#.VT9CTtGdKM8, retrieved on 10.04.2015.

[57] Pepe Escobar, *The Birth of the 'De-Americanized' World. Beijing Calls for Creation of New 'Reserve Currency' to Replace the US Dollar*, *Asian Times*, 15.10.2013, in Global Research, http://www.globalresearch.ca/the-birth-of-the-de-amercanized-world-beijing-calls-for-creation-of-new-reserve-currency-to-replace-the-u-s-dollar/5354330/, retrieved on 17.11.2013.

to establish the *New Development Bank* was signed in Fortaleza, Brazil; through this initiative, the five *"states of the future"*, a phrase coined by Chinese President, Xi Jinping, intend to *"democratise international relations"*, stating that the bank is destined for all the developing states to finance infrastructure projects[58];

- the installation of some medium-range missiles in Kaliningrad Oblast[59] and of some strategic fighters in the Crimean Peninsula[60];
- the military parade organised by Russia, in Moscow, on 9 May 2015, on the occasion of celebrating 70 years since the victory against the Nazi, was a true show of force as about 16,000 Russian troops[61] and some military contingents from China[62], India[63] and other 10 states participated in it, and cutting-edge combat assets and technology were displayed[64];
- the attempts at discrediting and even destabilising NATO through the rapprochement with Turkey – an Alliance member state –, to which Russia sells surface-to-air S-400 missiles, resulting in the USA warning of excluding Ankara from the 5th generation F-35 aircraft delivery programme[65];

The military parade organised by Russia, in Moscow, on 9 May 2015, on the occasion of celebrating 70 years since the victory against the Nazi, was a true show of force as about 16,000 Russian troops and some military contingents from China, India and other 10 states participated in it, and cutting-edge combat assets and technology were displayed.

[58] Astrid Prange, *BRICS Launch New Bank and Monetary Fund*, *Deutsche Welle*, 16.07.2014, http://www.dw.de/brics-launch-new-bank-and-monetary-fund/a-17789608, retrieved on 10.05.2015.

[59] Vasudevan Sridharan, *Moscow Moving Nuclear-capable Weapons to NATO Borders amid Massive Military Drills across Russia*, *International Business Time*, 18.03.2015, http://www.ibtimes.co.uk/moscow-moving-nuclear-capable-weapons-nato-borders-amid-massive-military-drills-across-russia-1492481, retrieved on 11.05.2015.

[60] *Russia Deploying Strategic Bombers to Crimea, Missiles to Kaliningrad*, Radio Free Europe, Radio Liberty, 17.03.2015, http://www.rferl.org/content/russia--strategic-bombers-crimea-missiles-kaliningrad/26906157.html, retrieved on 11.05.2015.

[61] Thomas Burrow and Will Stewart, *Now Russia's Got SEALS too. Armed Sea Creatures Show off Their Shooting Skills at Russia's Bizarre VE Day Parade*, Mail Online, 10.05.2015, http://www.dailymail.co.uk/news/article-3074519/Putin-Tanks-rumble-Red-Square-Russia-stages-biggest-Victory-Day-military-parade-Western-leaders-stay-away.html, retrieved on 11.05.2015.

[62] Mughda Variyar, *Moscow Victory Day Parade: Indian, Chinese Soldiers Go on Boat Rides, Sight-Seeing Together in Russia*, *International Business Time*, 09.05.2015, http://www.ibtimes.co.in/moscow-victory-day-parade-indian-army-contingent-marches-chinas-pla-631860, retrieved on 11.05.2015.

[63] *Indian Army Men Attract All Eyes during Russian Victory Day*, NDTV, 10.05.2015, http://www.ndtv.com/india-news/indian-army-men-attract-all-eyes-during-russian-victory-day-761836, retrieved on 11.05.2015.

[64] Mathew Chance and Laura Smith-Spark, *Russia Marks 70 Years since Victory over Nazi Germany with Huge Parade*, CNN, 09.05.2015, http://edition.cnn.com/2015/05/09/europe/russia-victory-day-celebration/, retrieved on 10.05.2015.

[65] Ted Galen Carpenter, *Is It Time to Expel Turkey from NATO?*, The National Interest, https://nationalinterest.org/blog/the-skeptics/it-time-expel-turkey-nato-14518, retrieved on 09.04.2019.

ROMANIAN MILITARY THINKING

- in the relations with the EU, the Russian Federation makes efforts to break the economic-financial blockade established by the Union, initiating bilateral economic-financial relations with Hungary, Slovakia, the Czech Republic[66], Germany[67] and Bulgaria[68];
- the correlation of certain political-diplomatic, economic-financial and military actions[69] with China in order to counter the similar actions conducted by the Western states against them[70].

3.1.4. Differences between the East-West Confrontations during the Cold War Period and the Current One

During the Cold War period, the USA and the USSR influenced the evolution of the international relations between most of the states in the world, not only between those in their spheres of influence. Currently, the USA and the USSR have less influence over international relations as new competitors in the struggle for world dominance have emerged – China, India, Brazil.

The current world order is no longer a bipolar one, being in transition from unipolarity to multipolarity.

During the Cold War period, the USA and the USSR influenced the evolution of the international relations between most of the states in the world, not only between those in their spheres of influence. Currently, the USA and the USSR have less influence over international relations as new competitors in the struggle for world dominance have emerged – China, India, Brazil.

Russia is considered a state having an authoritarian leadership, but it does not have the international span the USSR used to have and it does not practice the export of revolution as the Kremlin leadership used to do before 1990. Even though the Western world and Russia have different opinions related to the new world order and the way states should be organised and led in political and economic terms, the mentioned situation cannot be considered an ideological confrontation and a new Cold War[71].

[66] Tatia Dolidze, *EU Sanctions Policy towards Russia: The Sanctioner-Sanctionee's Game of Thrones*, 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 10.04.

[67] Yuriy Vitrenko, *Russia Weaponizing Gas*, Politico.eu, 4/29/19, https://www.politico.eu/sponsored-content/russia-weaponizing-gas/, retrieved on 12.05.2019.

[68] *Russia's Proposed TurkStream 2 Pipeline Sparks Bulgaria*, EU energy worries, Deutsche Welle, 28.02.2019, https://www.dw.com/en/russias-proposed-turkstream-2-pipeline-sparks-bulgaria-eu-energy-worries/a-47726458, retrieved on 10.05.

[69] Ben Blanchard, *China, Russia to Hold Joint Mediterranean Naval Drills in May*, Reuters, 30.04.2015, http://www.reuters.com/article/2015/04/30/us-china-russia-military-idUSKBN0NL16F20150430, retrieved on 15.05.2015.

[70] Timothy Heritage and Vladimir Soldatkin, *Putin Looks to Asia as West Threatens to Isolate Russia*, Reuters, 21.03.2014, http://www.reuters.com/article/2014/03/21/us-ukraine-crisis-russia-insight-idUSBREA2K07S20140321, retrieved on 03.01.2015.

[71] Odd Arne Westad, *Has a New Cold War Really Begun?*, Belfer Center, Harvard Kennedy School for Science and International Affairs, 27 March 2018, https://www.belfercenter.org/publication/has-new-cold-war-really-begun, retrieved on 17.07.2019.

Although Russia initiated a number of alliances following 1990, it is not supported by *"satellite states"* as it was the case of the USSR.

romania2019.eu

All the states in Eastern Europe that used to be Warsaw Pact member states, led by communist regimes, and considered Moscow satellite states, are now democratic states and NATO member states.

The North Atlantic Alliance is the most powerful political-military alliance in the world and it outpaces the Russian Federation in political, diplomatic, economic, financial, information, cultural and demographic terms. As for the military field, NATO also outpaces Russia in many respects, except for the nuclear one. In this respect, it can be said they are equal, considering that each of them has available a nuclear arsenal that could destroy life on Earth several times.

4. Conclusions

If, at the beginning of the Ukraine crisis, Russian President, Vladimir Putin, rejected the idea of a new Cold War, he has recently stated that "the West pushes us into confrontation"

Although many of the important Western leaders exclude the possibility of a new Cold War breakout, the way in which the East-West relations are conducted somehow contradicts this position.

If, at the beginning of the Ukraine crisis, Russian President, Vladimir Putin, rejected the idea of a new Cold War[72], he has recently stated that *"the West pushes us into confrontation"*[73].

The tendency towards confrontation in the East-West relations seems to be contagious as many states adopt relations based on the logic of the "*law of retaliation*". I mention but a few of the most recent ones: Saudi Arabia-Canada[74], USA-China[75], Japan-South Korea[76], China-Canada[77], Turkey-USA[78], Israel-Arab states etc.

[72] Konstantin Fets, *Russia Has No Intention of Building a New Iron Curtain, Says Putin*, *Russia beyond the Headlines*, 24.11.2014, http://rbth.co.uk/politics/2014/11/24/russia_has_no_intention_of_building_a_new_iron_curtain_says_putin_41637.html, retrieved on 03.02.2015.

[73] Serghei Lavrov, *Relațiile dintre Rusia și Occident sunt mai tensionate decât în perioada Războiului Rece*, Mediafax, 17.04.2018, http://www.mediafax.ro/externe/serghei-lavrov-relatiile-dintre-rusia-si-occident-sunt-mai-tensionate-decat-in-perioada-razboiului-rece-17133181, retrieved on 17.04.2018.

[74] Canadian Press, *Saudi Retaliation against Canada during Feud Detailed in Government Memo*, CBC News, 5 April 2019, https://www.cbc.ca/news/politics/saudi-retaliation-canada-memo-1.5085832, retrieved on 12.04.2019.

[75] *What Is a Trade War between US and China?*, Explained, Economyria.com, 22 June 2018, http://economyria.com/the-trade-war-between-the-us-and-china**/**, retrieved on 19.04.2019.

[76] Duncan Deaeth, *Japan Considers Economic Retaliation in Row with South Korea*, Taiwan News, 2019/03/14, https://www.taiwannews.com.tw/en/news/3657880, retrieved on 14.04.

[77] Amanda Connoly, *Detention of Canadians by China Was 'Retaliation' for Meng Arrest: Former U.S. Envoy to China*, Global News, 27 January 2019,https://globalnews.ca/news/4889420/xi-jinping-china-detentions-meng-wanzhou-gary-locke/, retrieved on 15.04.2019.

[78] Angela Dewan and Gul Tuysuz, *Why Turkey-US Tensions Have Come to a Boil*, CNN, 12 October 2017, https://edition.cnn.com/2017/10/12/politics/turkey-us-relations-explainer/index.html, retrieved on 10.04.2019.

ROMANIAN MILITARY THINKING

Experts in international relations and in information operations consider that the Cold War has not actually ended[79] but it is in its subversive phase[80] and, currently, it tends to resurface. In this regard, Michel Meyer states that it takes a long period of time to put an end to the Cold War as a change in the mindset is necessary, which cannot be made overnight[81].

BIBLIOGRAPHY

1. Madeleine Albright, *Doamna secretar de stat. Memorii*, Editura Rao, București, 2008.
2. Madeleine Albright, *Who Broke the U.N.*?, *Foreign Policy*, 13.08.2012, http://foreignpolicy.com/2012/08/13/who-broke-the-u-n/.
3. Fred C. Bergsten, *Japan and the United States in the New World Economy,* published by Theodore Rueter in *The United States in the World Political Economy,* Mc Graw-Hill, New York, 1994.
4. Clemens Bilan, *German MP: Russia's Exclusion from G8 "Wrong from Very Beginning"*, Sputnik News, 05.01.2016, https://sputniknews.com/politics/201601051032705436-germany-g8-russia/.
5. Michael Birnbaum, *Fearing Russian Expansion Baltic Nations Step up Military Exercises*, in *The Washington Post*, 16.05.2015, http://www.washingtonpost.com/world/europe/fearing-russian-expansion-baltic-nations-step-up-military-exercises/2015/05/15/b5ee51ee-f8c8-11e4-a47c-e56f4db884ed_story.html.
6. Goran Buldioski, *EU Must Confront Poland and Hungary*, EUObserver, Budapest, 21 November 2017, https://euobserver.com/opinion/139942.
7. Louis Charbonneau, *Russia Threatened Countries ahead of UN Vote on Ukraine, Diplomats Say*, Reuters, 28.03.2014, http://www.huffingtonpost.com/2014/03/28/exclusive-russia-ukraine_n_5052313.html.
8. 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/.
9. Teodor Danalache, *Ochi pentru ochi, dinte pentru dinte!*, Crestin Ortodox.ro, 30 July 2009, https://www.crestinortodox.ro/religiile-lumii/iudaism/legea-talionului-125032.html.
10. Ben Farmer, *I Can Take Kiev in Two Weeks, Vladimir Putin Warns European Leaders*, in *The Telegraph,* 01.09.2014, http://www.telegraph.co.uk/news/worldnews/ukraine/11069070/I-can-take-Kiev-in-two-weeks-Vladimir-Putin-warns-European-leaders.html.
11. Konstantin Fets, *Russia Has No Intention of Building a New Iron Curtain, Says Putin*, *Russia beyond the Headlines*, 24.11.2014, http://rbth.co.uk/politics/2014/11/24/russia_has_no_intention_of_building_a_new_iron_curtain_says_putin_41637.html.
12. Laurence Freedman, *The Cold War. A Military History*, Cassell & Co, London, United Kingdom, 2001.
13. Francis Fukuyama, *America la răscruce*. *Democrația, puterea şi moştenirea neoconservatoare*, Editura Antet XX Press, Filipeştii de Târg, Prahova, 2006.
14. Alistar Heath, *Tit-for-Tat Trade War with Russia Will Hurt Many but Achieve Little*, in *The Telegraph*, 7 August 2014, https://www.telegraph.co.uk/finance/economics/11020242/Tit-for-tat-trade-war-with-Russia-will-hurt-many-but-achieve-little.html.
15. Michael D. Hull, *The Big Three in Tehran: The Meeting that Shaped WWII*, Warfare History Network, 12 December 2018, https://warfarehistorynetwork.com/daily/wwii/the-big-three-in-tehran-the-meeting-that-shaped-wwii/.
16. Henry Kissinger, *Diplomația*, Editura BIC ALL, Bucureşti, 2007.
17. Olga Krasnyak, *Tit-for-Tat: Diplomatic Expulsions and Closures*, Center of Public Diplomacy (CPD), 13 September 2017, https://www.uscpublicdiplomacy.org/blog/tit-tat-diplomatic-expulsions-and-closures.
18. Serghei Lavrov, *Relațiile dintre Rusia şi Occident sunt mai tensionate decât în perioada Războiului Rece*, Mediafax, 17.04.2018, http://www.mediafax.ro/externe/serghei-lavrov-relatiile-dintre-rusia-si-occident-sunt-mai-tensionate-decat-in-perioada-razboiului-rece-17133181.
19. Jason Lemon, *New Russian Weapons "Significantly Increase" Military's Potential, Putin Warns Rivals*, Newsweek, 12/18/18, https://www.newsweek.com/russian-weapons-military-potential-putin-warns-1262973.
20. Edward Lucas, *The New Cold War: Putin's Russia and the Threat to the West*, 17 March 2009.
21. Pierre Milza and Serge Berstein, *Istoria secolului XX*, vol. 2, Editura BIC All, București, 1998.

[79] Sergei Karaganov, *Ukraine Crisis: the Cold War Never Really Ended,* in *The Telegraph*,06.05.2014, http://www.telegraph.co.uk/sponsored/rbth/opinion/10810159/ukraine-crisis-cold-war.html, retrieved on 10.08.2014.

[80] Keith Rogers, *Quiet Arms Race Continues, Retired CIA Officer Says,* in *Las Vegas Review Journal*, 17 March 2013, http://www.reviewjournal.com/news/military/quiet-arms-race-continues-retired-cia-officer-says, retrieved on 02.10.2013.

[81] Michal Meyer, *Has the Cold War Ended? Freedom from Fear*, no. 5, November 2009, pp. 38-39.

22. Alessandra Minerbi, *Istoria ilustrată a nazismului*, Editura Rao, Bucureşti, 2006.
23. Aamna Mohdin, *Populist, Authoritarian Leaders Are Still on the Rise across Europe*, Quartz, 12 July 2017, https://qz.com/1027518/populist-authoritarian-leaders-are-still-on-the-rise-across-europe/.
24. John McNeer, *The Space Race in the Context of the Cold War*, History Arch, 20 July 2018, https://historyarch.com/2018/07/20/the-space-race-in-the-context-of-the-cold-war/.
25. Arnold A. Offner, *President Truman and the Origins of the Cold War*, BBC http://www.bbc.co.uk/history/worldwars/wwtwo/truman_01.shtml.
26. Julie Pace and Matthew Lee*, Hoping to Isolate Russia, US Woos China on Ukraine, Associated Press,* 11.03.2014, http://www.irrawaddy.org/asia/hoping-isolate-russia-us-woos-china-ukraine.html.
27. Thomas Parish, *Enciclopedia Războiului Rece*, Editura Univers Enciclopedic, Bucureşti, 2002.
28. William Pfaff, *The Question of Hegemony*, *Foreign Affairs*, January-February 2001, http://www.foreignaffairs.com/articles/56654/william-pfaff/the-question-of-hegemony.
29. Roberta Rampton, *Biden Warns Russia Will Be Isolated If Ukraine Crisis Not Resolved: US Official*, *Reuters*, 3 March 2014, http://news.yahoo.com/biden-warns-russia-isolated-ukraine-crisis-not-resolved-174333462.html.
30. Scott Michael Rank (editor), *Winston Churchill's Iron Curtain Speech: Predicting the Cold War, History on the Net*, https://www.historyonthenet.com/winston-churchills-iron-curtain-speech-predicting-the-cold-war.
31. Ronald Steel, *Temptations of a Superpower*, Harvard University Press, 1995.
32. Simon Tisdall, *The New Cold War: Are We Going Back to Bad Old Days?*, in *The Guardian*, 19.11.2014, http://www.theguardian.com/world/2014/nov/19/new-cold-war-back-to-bad-old-days-russia-west-putin-ukraine.
33. Mark Thompson, *Russian Forces Double along Ukraine Border*, Time, 28.03.2014, http://time.com/41490/russia-ukraine-crimea-putin/.
34. Simon Trewand Garry Sheffield, editors, *100 Years of Conflict 1900-2000*, Sutton Publishing Limited, Phoenix Mill, UK, 2000.
35. Mughda Variyar, *Moscow Victory Day Parade: Indian, Chinese Soldiers Go on Boat Rides*, Sight-Seeing Together in Russia, International BusinessTime,09.05.2015,http://www.ibtimes.co.in/moscow-victory-day-parade-indian-army-contingent-marches-chinas-pla-631860.

36. Shaun Walker, *Dmitry Medvedev Visits Crimea as Russia's Army Begun Border Withdrawal*, in *The Guardian*, 31.03.2014, http://www.theguardian.com/world/2014/mar/31/dmitry-medvedev-crimea-army-border-withdrawal-ukraine.
37. H. P. Willmott, *The Second World War in the Far East*, Cassell & Co, Wellington House, London, 1999.

NEW TECHNOLOGIES – RISKS AND VULNERABILITIES FOR THE NATIONAL SECURITY. CYBERTERRORISM

Anca SAVU
PhD candidate, "Carol I" National Defence University, Bucharest
Florentina-Ştefania NEAGU
PhD candidate, "Carol I" National Defence University, Bucharest

Not long ago, the emergence of the Internet and the development of new technologies promised to provide us with a global infrastructure, extremely easy and comfortable to use, that would bring us the facilities of the real world right in front of the computer, a click away. Today, new technologies can be used in the development of new successful business models, as tools in political struggle, as well as in espionage, military operations and, most importantly, they have become a major vector for the spread of cyber attacks.

The international security environment is becoming increasingly uncertain, and cyber vulnerabilities play an important role in its deterioration. This is why knowing the level of development of new technologies is of particular importance, especially in the context in which the protection of national information systems targeted by hacker groups or non-state entities has become a major concern, as evidenced by the national security documents of countless countries in the world.

Keywords: cyber attack, new technologies, intelligence agencies, terrorism, security.

romania2019.eu

Introduction

The Internet appeared, as a functional idea, in the technological laboratories of the US Army, in the seventh decade of the last century, so that in the 1990s the world wide web developed by the British Tim Berners-Lee[1] would begin to conquer the world. Most of the daily activities involve the use of the Internet today: through it you can control all the computer systems, from the personal computer to the monitoring of the national electricity networks and the traffic on the big arteries of the capitals of the world.

Today, new technologies emerging in the age of the Internet include a multitude of types of gadgets, data collection and interpretation software, e-learning platforms, medical devices based on 3D technology, cars without a driver, computers that can make payments only through smile scanning and more. Already artificial intelligence is widely used in the car industry, as well as in the construction of new and extremely sophisticated weapons. The term *"artificial intelligence" (AI)* was first used by American professor John McCarthy in 1956, and in terms of the definitions used, they are innumerable, but all refer to the ability of a machine to use it in a way autonomous logical, rational computational models, like algorithms or different statistical models, and have the same meaning: *"the art of creating machines that perform functions that would require intelligence if they were performed by humans"*[2]. However, there is a common denominator, namely that any device that is considered to be equipped with artificial intelligence should pass

New technologies emerging in the age of the Internet include a multitude of types of gadgets, data collection and interpretation software, e-learning platforms, medical devices based on 3D technology, cars without a driver, computers that can make payments only through smile scanning and more. Already artificial intelligence is widely used in the car industry, as well as in the construction of new and extremely sophisticated weapons.

[1] Tim Berners-Lee is a British programmer, credited with inventing the web. Born in 1955, he graduated from Oxford University in 1976. In 1989, as an employee of CERN, he laid the foundations of what we now call the world wide web, for the first time proposing a system of information management at the global level. Tim Berners-Lee made at CERN, HTTP (HyperText Transfer Protocol), HTML (HyperTextMarkup Language), the first web browser named "World Wide Web", the first HTTP server software (Httpd CERN), the first website and web server, info.cern.ch, available at https://www.britannica.com/biography/Tim-Berners-Lee.

[2] *Inteligența artificială: ce este și cum funcționează*, available at https://www.stiintaonline.ro/inteligenta-artificiala-ce-este-si-cum-functioneaza/

ROMANIAN MILITARY THINKING

the *"Turing test"*, which seeks to answer the difficult question of whether machines can think[3]. Although the person who proposed this test, British mathematician Alain Turing, predicted that by the year 2000 it would be passed by a human-created device, this did not happen.

A very important factor in the evolution of new technologies was the simplified access to the calculation technique. Basically, today it is hard to find a home or office without a smart device or personal computer. And the trend is still growing, after decades of development of computer programmes and connections that have led to the improvement of computers due to the large and constant investments by companies in the development of this field, as well as the availability of data storage spaces or the implementation of techniques working with systems based on artificial intelligence.

Taking into account the fact that technologies are very important for any state, irrespective of its level of development, both the benefits and the risks that they may pose for institutions in the field of national security will be presented in the article. In the same note, the way in which these technologies can be used by some groups in order to initiate cyber attacks will be addressed.

The term cyberterrorism was first defined by researcher Barry Collin of the California Institute of Security and Information in the 1980s, as follows: "cyberterrorism represents the convergence between cyber space and terrorism". This convergence refers to the illegal attacks on computers, networks and information stored there, when they are made to intimidate or constrain a government or its employees in promoting political or social goals.

Cyberterrorism

The term cyberterrorism was first defined by researcher Barry Collin of the California Institute of Security and Information in the 1980s, as follows: *"cyberterrorism represents the convergence between cyber space and terrorism"*[4]. This convergence refers to the illegal attacks on computers, networks and information stored there, when they are made to intimidate or constrain a government or its employees in promoting political or social goals. Moreover, in order to qualify as cyberterrorism, an attack should lead to violence against people to generate a state of fear[5].

[3] http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

[4] B. Collin, *The Future of Cyber Terrorism*, Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996.

[5] N. Bradley, *Cyberterrorism Is Real – Is It?*, Twickelerveld Intelligence and Investigations, available at http://www.intelligence-and-investigations.com/media/uploads/62_Cyberterrorism%20-%20Nicholas%20Bradley.pdf

Dorothy Denning, a cyber security expert, defines cyberterrorism as those *"politically motivated hacking operations designed to cause major damage, such as loss of life or serious economic harm"*[6].

romania2019.eu

Cyberterrorism is one of the vulnerabilities faced by a state and could result in violations of national security, as well as losses of physical, digital, financial assets, which would cause the population's confidence in state institutions to decline. Such intervention can be manifested through various forms, such as: interruption of services considered vital, identity theft, improper use of control systems in managing the physical transport infrastructure and disruption of car, rail or air traffic attacking security filters etc. There are just a few examples, to which computer crime activities can be added, such as theft of information in order to obtain money from them[7].

Cyberterrorism is one of the vulnerabilities faced by a state and could result in violations of national security, as well as losses of physical, digital, financial assets, which would cause the population's confidence in state institutions to decline.

At the global level, there are currently two trends of cyber attacks, the first type including political acts aimed at producing damages, especially at the level of the collective mind. These are similar to the acts of conventional terrorism, as were the attacks on some Danish websites, in response to the caricatures of Prophet Muhammad published by a Danish newspaper. The second type are actions lacking political purpose but based on information and communication technology and implemented by hackers, such as DDoS[8] virus attacks, blackmail and unauthorised access to private, corporate or government systems with the intention to view, copy confidential data, etc[9].

There are also large attacks. In August 2012, Saudi Aramco suffered a major cyberattack, which resulted in the shutdown of 30,000 computers. The company's computer network was infected with a virus, in an unprecedented act of sabotage. The attack was claimed by a group called the Justice Cutting Sword, which accuses

[6] D. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, in J. Arquilla and D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militacy*, Rand, Santa Monica, available at http://www.nautilus.org/info-policy/workshop/papers/denning.html

[7] A. De Borchgrave, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, CSIS Homeland Defense Project, CSIS Pres, Washington, D.C., 2001.

[8] Distributed Denial of Service (DDoS) is an attack on a computer or relay meant to reduce, restrict or prevent access to its resources by legitimate users. In such an attack the attackers flood the victim's system with requests for services or traffic to overload resources, according to https://askit.ro/solutii/ce-inseamna-un-atac-dosddos-si-ce-impact-are/

[9] M. Gorge, *Cyberterrorism: Hype or Reality?*, in *Computer Fraud & Security*, 9-12, 2007, available at https://www.researchgate.net/publication/223089895_Cyberterrorism_hype_or_reality

ROMANIAN MILITARY THINKING

the Saudi government of crimes and atrocities in several countries. The virus caused data to be erased for three quarters of the company's computers, replacing it with the image of a burned American flag. After this attack, the Gulf states became more receptive to such acts of sabotage on national companies[10].

Various studies and reports prepared by international organisations have shown that cyber terrorists use the internet as a means of conducting hostile activities, which has led to the development of a strategic framework and policies to combat cyberterrorism[11].

To highlight the impact of a cyber attack on a vital area of a country's economy, such as the energy one, an eloquent example is the situation of the American energy company Enron, which, under false pretences, shut down a power plant, raising energy prices and generating high profit for the company. In the most pessimistic scenario, if a hacker attacks the cyber system that controls the activity of a power plant or nuclear power plant, the effects would be dramatic.

Use of technology to initiate cyber attacks

Technology has invaded our lives, often even without suspicion. In the near future, increasing automation and innovation will affect employment by developing industries that today rely on large numbers of staff, because the implementation of automated devices, although generating higher costs at first, is amortized relatively quickly, and efficiency is customized.

In this context, to highlight the impact of a cyber attack on a vital area of a country's economy, such as the energy one, an eloquent example is the situation of the American energy company Enron, which, under false pretences, shut down a power plant, raising energy prices and generating high profit for the company[12]. In the most pessimistic scenario, if a hacker attacks the cyber system that controls the activity of a power plant or nuclear power plant, the effects would be dramatic.

In order to prevent and counter such actions, which can easily be included in the chapter on cyber-terrorism, a considerable effort of specialised services is needed. A starting point is the collection of data from social networks, but also from surveillance systems (such as infrared sensors, motion detectors, low power radars and persistent

[10] BBC, *Saudi Aramco Oil Giant Recovers from Virus Attack News Technology*, 27 August 2012, available at https://www.bbc.com/news/technology-19389401.

[11] Z. Yunos, *Putting Cyberterrorism into Context*. STAR In-Tech, available at http://www.cybersecurity.my/data/content_files/13/526.pdf?.diff=1236049327, 2009.

[12] M. Tran, S. Khaw, The man who founded Enron, Kenneth Lay, has died just weeks before his jail sentence was to be announced. Mark Tran and Stefanie Khaw look at one of America's biggest business scandals, 6 July 2006, available at https://www.theguardian.com/business/2006/jul/06/corporatefraud.enron.

surveillance technologies that combine image with powerful digital signal processing[13]). Annually, databases store an impressive amount of information, which is a challenge for information services in terms of automating the process of data collection, structuring and filtering[14].

romania2019.eu

The evolution of the IT domain in the last few years has led the information services from all over the world to implement efficient data collection and analysis systems to keep up to date with the information that is circulating very quickly and in huge amounts in social media. Such an approach was made by the US Air Force Research Laboratory, which announced in 2014 the launch of the MUSIENA (Multi-Source Information Extraction & Network Analysis) program. This program seeks to develop analytical tools, algorithms and projects to help the US Air Force, as well as other intelligence analysts, access and quickly analyse large amounts of data to discover and identify military threats, as well as other threats types to national security, including acts of cyberterrorism[15].

The evolution of the IT domain in the last few years has led the information services from all over the world to implement efficient data collection and analysis systems to keep up to date with the information that is circulating very quickly and in huge amounts in social media.

All this takes place in the context in which the terrorist group Islamic State is active on almost all social networks, plus the fact that it has its own media structures. In addition to this organization, other organizations are active on social networks as well as in the *"Dark Net"*[16]: Hamas (Islamic Resistance Movement), Lebanese Hezbollah (God Party), the People's Revolutionary Liberation Front Party in Turkey (DHKP-C), Kurdistan Workers' Party (PKK), Uzbekistan Islamic Movement (IMU) etc.

In the study published in 2015 by Professor Gabriel Weimann, from the University of Haifa, Israel, called *"Terrorism in Cyberspace: The Next Generation"*, he demonstrated that, since 1998, the presence of terrorists on the Internet had increased. Thus, in 1998, the number of websites containing terrorist material was 12, in 2003 there were

[13] J. Keller 2015, *The Growing Role of Technology in the Global War on Terrorism*, 8 December 2015, available at http://www.militaryaerospace.com/articles/2015/12/counter-terrorism-technology.html.

[14] I. Bodolan, *Impactul noilor tehnologii asupra procesului de intelligence*, 7 November 2012, available at http://intelligence.sri.ro/impactul-noilor-tehnologii-asupra-procesului-de-intelligence/

[15] J. Keller, *The Growing Role of Technology in the Global War on Terrorism*, 8 December 2015, available at http://www.militaryaerospace.com/articles/2015/12/counter-terrorism-technology.html.

[16] *The Role of Technology in Modern Terrorism*, 3 February 2016, available at http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref

2,650 pages with this profile, and in September 2015 the total number reached 9,800[17].

The new technologies, but also the Internet, can be used for many purposes, such as: propaganda, psychological warfare, recruitment and mobilisation, fundraising, Data Mining, information collection, encrypted communications, cyber attacks, distribution of Islamist materials through applications mobile, the purchase of fake documents. Since 2013, the Islamic State group has developed several Android operating system applications for encrypted communications between members of the organisation. Also, the group is trying to recruit young hackers who are motivated by earning some money, but also by the interest the organisation shows towards their skills.

An increasing concern for intelligence services is the fact that terrorists disseminate radical messages or interactive videos and animations to highly vulnerable target groups, such as children and adolescents. Also, applications such as Google Maps or Google Earth, provide terrorists with a wealth of detailed information about the goals – potential targets, within a country.

An increasing concern for intelligence services is the fact that terrorists disseminate radical messages or interactive videos and animations to highly vulnerable target groups, such as children and adolescents. Also, applications such as Google Maps or Google Earth, provide terrorists with a wealth of detailed information about the goals – potential targets, within a country.

Starting with 2013, the Islamic State group has developed several applications for the Android operating system meant for encrypted communications between organisation members. Moreover, the group has been trying to recruit young hackers who are driven by the prospect of making good money, as well as by the interest shown by the organisation in their skills. And the fact that some of them are speakers of rare dialects such as Urdu, Tamil, Telugu, Malayalam, Kannada, etc., contributes to the propagation of radical messages on a digital area as wide as possible.

The effects of using artificial intelligence and information technology by cyber terrorists on national security

The face-recognition systems developed since 2015 by Microsoft and Google were immediately integrated by the CIA and FBI in the United States and, subsequently, by the other intelligence services, which were of great help in the initial phase because they could lead to the identification of criminals. In 2017, Apple introduced facial

[17] *Ibid*.

recognition software into its phones, which will create a vulnerability for both information services and phone users, as it corroborates the information that can be extracted from the applications that the phones have embedded they can lead to 100% identification of an individual. The most common biometric applications that gadgets have are: finger prints, hand geometry, biometric retinal authentication, facial recognition as well as keyboard rhythm recognition[18].

On the other hand, applications that rely on artificial intelligence are useful not only for data analysis, but also for content generation, such as: realistic modification of facial expressions, real-time mouth movements, creation of real voice recordings, image production false according to the text description, the production of written news articles based on structured data such as political data, polls, election results, financial reports, etc[19].

In the long term, AI-based technologies are useful not only for analysing data from multiple sources and integrating them to reach some conclusions intended to support the recipient of the intelligence product, but also to generate false conclusions. In other words, these technologies can help intelligence services to extract accurate information, but also to provide misinformation to the adversary in order to cause it to change its strategy.

In the long term, AI-based technologies are useful not only for analysing data from multiple sources and integrating them to reach some conclusions intended to support the recipient of the intelligence product, but also to generate false conclusions. In other words, these technologies can help intelligence services to extract accurate information, but also to provide misinformation to the adversary in order to cause it to change its strategy.

These technologies can support totalitarian regimes or overthrow governments as was the case in the Arab Spring, when the population of the Maghreb states mobilized to take to the streets. During the Tunisian uprising, the online environment and, above all, blogs, were almost the only sources of information, photos and video images for street fighting. The transmission of UGC (User Generated Content) has become almost an act of conduct for reporting news from ongoing events, as conventional media could not have access or the necessary means.Blogs and the transmission of photos and video images through mobile phones have become the main sources of dissemination and consumption of news about street protests[20].

[18] R. Bandakkanavar, *Introduction to Biometric Technology*, 10 September 2017, available at https://krazytech.com/technical-papers/biometric-technology.

[19] G. Allen, T. Chan, *Artificial Intelligence and National Security*, Cambridge: Belfer Center for Science and International Affairs-Harvard Kennedy School, 2017, p.29.

[20] D. Cristea, *Rolul tehnologiilor informatice şi de comunicaţii în desfăşurarea revoltelor din Primăvara Arabă*, in *Revista Comunicaţiilor şi Informaticii*, no. 1, 2012, pp. 60-61.

ROMANIAN MILITARY THINKING

Moreover, fake news that is disseminated with the help of new communication technologies will put media organisations or think tanks at a standstill. They will even report fake news as being real, as the process of verifying news is complex, and events are proceeding at an alert pace. Most of the time, journalists and analysts evaluate information under time pressure, and the end result can lead to misinformation.

When it comes to driving multiple types of technologies to an unwanted event, the result is often very difficult to counteract by intelligence services. An example is the event that took place on 23 April 2013, in which hackers took control of the Associated Press Twitter account and posted a terrible announcement: "*BREAKING NEWS: Two explosions have taken place at the White House, and President Barack Obama is hurt*"[21]. In the next three minutes after the news was published, the Dow Jones index collapsed, and the US lost $ 136.5 billion on the stock market. This involved mobilising White House employees and the American political establishment to reassure the population and convince them that this was just fake news, and the president is unharmed.

Currently, there are open conflicts in countless places in the world, and these must be fed with weapons, sometimes of the newest and most efficient type. According to the report by Boston Consulting Group for the period 2000-2015, global spending on military robotics (which refers strictly to unmanned vehicles) has tripled from $ 2.4 billion to $ 7.5 billion and is expected to exceed 16 billions of dollars by 2025.

The effect of technological development for military affairs. Possible scenarios

Currently, there are open conflicts in countless places in the world, and these must be fed with weapons, sometimes of the newest and most efficient type. According to the report by Boston Consulting Group for the period 2000-2015, global spending on military robotics (which refers strictly to unmanned vehicles) has tripled from $ 2.4 billion to $ 7.5 billion and is expected to exceed 16 billions of dollars by 2025[22].

As for the danger that technical innovation is exporting in the military field, it derives from the fact that new technologies are becoming cheaper, so accessible to almost anyone, not just military personnel. Most likely, in the next ten years, the advancement of technologies based on artificial intelligence will transform the armies.

[21] P. Foster, *Bogus' AP Tweet about Explosion at the White House Wipes Billions off US Markets*, 23 April 2013, available at http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

[22] G. Allen, T. Chan, *Artificial Intelligence and National Security,* Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017, p.14.

Most likely, more autonomy will be granted to the military through the assistance provided by the performing systems that are used in the theatres of operations. It will also accelerate the transition from air missions with human crew, to missions with unmanned aircraft.

In 2017, the BelferCenter for Science and International Affairs at Harvard Kennedy School conducted a study analysing 10 scenarios on how new technologies could transform a state's military power. We will present, in the following, some of these scenarios:

a) Lethal autonomous weapons will be part of the structure of military forces. In the Russian Federation, the Industrial Military Committee has approved a rather aggressive plan, whereby 30% of the military forces' capacity will be endowed with autonomous robotic platforms, and this plan will be implemented by 2030. These weapons will also solve a problem with some states are facing, namely the demographic decline that causes a much smaller number of young people to choose a military career.

b) The evolution of technologies makes the military platforms used today obsolete. Currently, large military drones have a much higher cost, and commercial drones have a limitation on the weight they can carry. Solutions are being sought for a military plane to deal with an attack by several drones that could lift explosive devices off the ground.

c) Assassinations produced by robots may become commonplace and difficult to attribute a person, entity, etc. The wide availability and low cost of component parts, combined with human inventiveness, can lead to the construction of robots much easier than a few years ago. Thus, in the present scenario, a small, autonomous robot could enter a home and lethally attack a human target leaving no traces.

d) *"Cyberweapons"* are commonly used to kill. Connecting digital and physical systems will increase the number of possibilities to kill with these weapons. A car will be able to be diverted and remotely controlled so as to cause a chain accident on the freeway. An example of this is possible is the case of the hacker Chris Roberts who, in 2015, managed to access the critical functions of an airplane, including the engine, through the entertainment system of the airplane[23].

romania2019.eu

One of these scenarios addresses the fact that lethal autonomous weapons will be part of the structure of military forces. In the Russian Federation, the Industrial Military Committee has approved a rather aggressive plan, whereby 30% of the military forces' capacity will be endowed with autonomous robotic platforms, and this plan will be implemented by 2030. These weapons will also solve a problem with some states are facing, namely the demographic decline that causes a much smaller number of young people to choose a military career.

[23] E. Perez, *FBI: Hacker Claimed to Have Taken over Flight's Engine Controls*, 25 May 2015, available at http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html.

ROMANIAN MILITARY THINKING

Two other vulnerabilities are: the Autopilot system, which is installed on board aircraft and which pilots use for long flights, and the automatic surveillance that most airlines use. By automatic surveillance, unencrypted data about the position of an aircraft is sent to the control tower. This data could be manipulated by a malicious person who could alter the actual positioning of an aircraft.

e) Unexpected interactions between autonomous systems can cause blockages. Due to the high operating speed of autonomous systems, they can get out of control. An example is the United States Flash Crash Stock Exchange, which announced a $1 billion loss in May 2010 due to unintended interaction of payment systems. This prompted the executive management to reassess the entire global stock exchange payment system[24].

Unexpected interactions between autonomous systems can cause blockages. Due to the high operating speed of autonomous systems, they can get out of control. An example is the United States Flash Crash Stock Exchange, which announced a $1 billion loss in May 2010 due to unintended interaction of payment systems. This prompted the executive management to reassess the entire global stock exchange payment system.

f) Theft and reproduction of military equipment or theft of confidential information. Stealing data plans and research and development of American fighter aircraft F-22 and F-35 by the Chinese is just one example of this, and not just aerospace industry is affected[25].

Counteracting cyber terrorism

Cyber threats are usually cross-border in nature, but the response to them is mostly national. A factual state that wants to be changed, at least at the level of the European Union. According to a document dealing with the topic of cyber security, annexed to the report on the state of the European Union in 2016[26], the number of *ransomware*[27] attacks increased by 300% between 2015-2016, reaching 4000 per day, and over 80% of European companies suffered the at least one cyber attack during 2016. The same document states, regarding the Internet of Things, that by 2020 there will be tens of billions of different digital devices connected to an already extremely busy network in the EU.

[24] M. Eggan, *Flash Crash: Could It Happen Again?*, 6 May 2014, available at http://money.cnn.com/2014/05/06/investing/flash-crash-anniversary/index.html

[25] Ling. J, *Man Who Sold F-35 Secrets to China Pleads Guilty*, 24 March 2016, available at https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.

[26] *Resilience, Deterrence and Defence: Building Strong Cybersecurity in Europe*, available at https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf.

[27] Ransom ware programs are malicious elements whose role is to encrypt files. The latter should be repurc hased later, with users paying hackers to regain access to its files, according to https://www.bitdfender.ro/support/new-functie-remediation-ransomware-in-bitdefender-2019-2216 .html

romania2019.eu

And if we add that in 2016 in some of the EU member states over 50% of the crimes were already cyber, the picture of vulnerability to cyber threats is already very bleak.

The EU response first came to fruition by adopting, in 2013, the EU Cyber Security Strategy, aimed at guiding policies to respond to these threats. The first EU cyber security legislative act was adopted in 2016 in the form of Directive 2016/1148 (NIS Directive), which laid down requirements on national cyber security capabilities, created the first mechanisms to enhance strategic and operational cooperation between member states and introduced security and incident orting[28] obligations in sectors vital to the economy and society, such as energy, transportation, supply and distribution ofdrinking water, banks, financial market infrastructures, healthcare, digital infrastructures, and service providers digital essentials.

The first EU cyber security legislative act was adopted in 2016 in the form of Directive 2016/1148 (NIS Directive), which laid down requirements on national cyber security capabilities, created the first mechanisms to enhance strategic and operational cooperation between member states and introduced security and incident reporting obligations in sectors vital to the economy and society.

In 2017, it followed the implementation of a set of measures established at the level of the European Commission, including the establishment of a Cyber Security Agency (ENISA), which will support the member states in this field, the establishment of a European cyber security certification framework for a series full of digital products, a quick response procedure in the event of a cyber attack, the creation of a network of cyber security research centres throughout the EU, the tightening of the law regarding the fraud of the Internet, as well as different measures to intensify the international cooperation, especially between the EU and NATO. All these measures were enacted at the end of 2018, when the European Parliament adopted the EU Cybersecurity Act[29].

ENISA, the spearhead of the EU in countering cyber threats, assists both EU institutions and the public and private sectors in the Member States. The Agency organises cyber security exercises, provides assistance for the development of national cyber security strategies,

[28] The responsible institution at EU level is CSIRT – Computer Security Incident Response Team. In our country, the contact point is the National Cyber Security Incident Response Center– CERT-RO, an institution under the coordination of the Ministry for the Information Society. Its main missions are to prevent, analyse, identify and respond to incidents occurring within cyber infrastructures that provide public utility functionality or information society services, according to https://www.cert.ro/?fbclid=IwAR1VX9NHWdkLt5mypj4vUcjKMAFhicRPBtrMoPBjXQlwBd2dIdPGURwivLM#

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

and contributes to the development of EU policy and legislation on network and information security. All stakeholders, from the public and private sectors, are part of a network that includes Europol and the European Center for the fight against cybercrime. The activity of this network focuses on the following elements:

- Expertise: anticipating the main emerging challenges related to network and information security, taking into account developments in the digital environment and supporting Europe in addressing them;
- Policy: support member states and EU institutions in developing and implementing the policies necessary to meet the legal and regulatory requirements regarding national information security;
- Capacity: support for the consolidation of state-of-the-art capabilities in terms of network and information security;
- Community: strengthening cooperation between member states and between bodies responsible for ensuring the security of information at national level[30].

All EU countries have a national cyber security strategy, to face the constant challenges of the ever-changing cyber environment. But the vulnerability is obvious and no example is more appropriate than Estonia, one of the most "digitised" countries in the world.

Today, all EU countries have a national cyber security strategy, to face the constant challenges of the ever-changing cyber environment. But the vulnerability is obvious and no example is more appropriate than Estonia, one of the most *"digitised"* countries in the world.

Massive deployment of network-based technologies began quite early in the Baltic country, as early as the mid-1990s, so ten years later it was listed as the most connected country in Europe. However, in the spring of 2007, following internal conflicts related to the government's attempt to move a statue of the Soviet era, which provoked the anger of the ethnic Russians, Estonia became, for 3 weeks, the target of a massive cyber-attack launched and coordinated it seems, from Russia. Between 27 April and 18 May 2007, a huge wave of DdoS-type attacks targeted the national digital infrastructure, managing to close all the websites of the ministries, two of the largest banks, as well as most of the political parties. The servers and other IT capabilities were paralysed for days, and critical infrastructures such as water or energy were in great danger. Although the involvement of the Kremlin

[30] https://europa.eu/european-union/about-eu/agencies/enisa_ro#cum-func%C8%9Bioneaz%C4%83

in these attacks could not be demonstrated, the fact that the Russian officials encouraged them, through the messages transmitted, is within the domain of evidence[31]. Unable to make full use of resources to counter the attack, the Estonian CERT team called for support from similar centres in Finland, Germany, Slovenia and Israel. NATO and the EU also intervened through the specialised bodies, so that the situation finally returned to normal.

The 2007 attack was a serious alarm signal not only for Estonia, but also for the entire international community, as it has been shown that any modern society is vulnerable to these threats. At national level, all the lessons learned were collected in an emergency regime and based on them the entire scaffolding of the Estonian cyber defence was reconstructed. New policies, new strategies, new concepts[32], including new specialised university programmes have made Estonia one of the safest countries in the world for such threats.

Directly following the 2007 attack, in January 2008, NATO approved the first policy of the Alliance in the field of cyber defence, and in May 2008, inaugurated, in Tallinn, the Center of Excellence in the field of cyber defence cooperation (CCDCOE), an institution providing expertise specialised to both NATO member states and partner countries. Also, cyber security was to be included in the 2010 Strategic Concept, which provided that NATO would defend the territory and population of the member states against all threats, including cyber threats[33].

In January 2008, NATO approved the first policy of the Alliance in the field of cyber defence, and in May 2008, inaugurated, in Tallinn, the Center of Excellence in the field of cyber defence cooperation (CCDCOE), an institution providing expertise specialised to both NATO member states and partner countries. Also, cyber security was to be included in the 2010 Strategic Concept, which provided that NATO would defend the territory and population of the member states against all threats, including cyber threats.

The year 2016 would mark two other extremely important issues: the commitment of the member states to strengthen their cyber defence at national level and to intensify cooperation in this field, a commitment made in the form of a document known as the Cyber

[31] Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, pp. 51-52, available at https://www.researchgate.net/publication/229014537_Revisiting_the_Estonian_Cyber_Attacks_Digital_Threats_and_Multinational_Responses

[32] Data Embassy and Blockchain are the main tools of Estonian *"fight"* against cyber threats. The first refers to the retention of national data on servers located in another country but remained under national jurisdiction (Luxembourg, in the case of Estonia), and the second to databases organized on blocks linked together and individually encrypted. Available at https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf, https://e-estonia.com/category/blockchain/

[33] *Defending the Networks*, *The NATO Policy on Cyber Defence,* available at https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

ROMANIAN MILITARY THINKING

Defense Pledge[34], as well as the recognition cyberspace as an operational domain, at the Warsaw Summit. In June 2018, a new programmatic document, entitled *"NATO Vision and Strategy on Cyberspace as a Domain of Operations"* was adopted, and by the end of 2019 the Alliance will also benefit from a doctrine related to this field.In 2023, the new NATO structure that will operationally manage this area, the Cyberspace Operations Center, based in Mons, Belgium, will reach the level of full operational capacity[35].

Conclusions

In order to counteract the new threats outlined in the newest dimension, the cyber dimension, new procedures and security policies are needed. However, the transformation of services will be a much more difficult process, as it involves in-depth changes based on future risk estimates, and the resistance to change is generally considerable, requiring a continuous and sustainable transformation.

From the examples presented, one can come to the conclusion that new technologies affect not only the areas vital to national security, but also the lives of each one of us. They are present today in every home and within the reach of any individual, and can be purchased at a low price due to the fierce competition on the profile market. New technologies offer a number of advantages, they make our lives easier and can be a prerequisite for healthy economic growth, if they are used to their full potential. In the field of national security, they can support the information services in collecting, analysing and disseminating information relevant to those entitled to make decisions on behalf of the station.

However, in the coming years, if the evolution of new technologies continues at the same pace, it will definitely lead to a profound transformation of intelligence services. In order to counteract the new threats outlined in the newest dimension, the cyber dimension, new procedures and security policies are needed. However, the transformation of services will be a much more difficult process, as it involves in-depth changes based on future risk estimates, and the resistance to change is generally considerable, requiring a continuous and sustainable transformation[36]. Of course there is only one thing, that our future will be in the hands of the one who will have the most developed technologies and who will at the same time be aware that he does not have a monopoly on them and will ensure that threats from the cyber space and beyond, can be counteracted.

[34] *Cyber Defence Pledge*, available at https://www.nato.int/cps/en/natohq/official_texts_133177.html.

[35] https://www.euractiv.com/section/defence-and-security/news/nato-sees-new-cyber-command-centre-by-2023-as-europe-readies-for-cyber-threats/.

[36] I. Grosu, *Serviciile de informații: Reformă sau transformare*, 26 July 2009, available at https://intelligence.sri.ro/serviciile-de-informatii-reforma-sau-transformare/.

romania2019.eu

Bibliography

1. ***, *EU Terrorism Situation and Trend Report*, EUROPOL, 2012, available at https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report.
2. ***, *MIT Technology Review*, 2017, available at MIT Technology Review: https://www.technologyreview.com/lists/technologies/2017/.
3. ***, *National Cyber Security Strategy Canada's Vision for Security and Prosperity in the Digital Age*, Government of Canada, 2018, available athttps://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s35.
4. ***, *Saudi Aramco Oil Giant Recovers from Virus Attack News Technology*, BBC, 27 August 2012, available at https://www.bbc.com / news /technology-19389401.
5. *"Suspect de terorism, declarat indezirabil",* SRI, 2 August 2017, available at www.sri.ro:https://www.sri.ro/articole/suspect-de-terorism-declarat-indezirabil-august -2017.
6. G. Allen, T. Chan, *Artificial Intelligence and National Security*, Cambridge: Belfer Center for Science and International Affairs-Harvard Kennedy School, 2017.
7. R. Bandakkanavar, *Introduction to Biometric Technology*, 10 September 2017, available at https://krazytech.com/technical-papers/biometric-technology.
8. P. Berkowitz, *The Future of American Intelligence*, 2005, Hoover Institution Press Publication.
9. S. Biddle, *How ISIS Makes Its Blood Sausage*, 2 June 2015, available at https://gawker.com/how-isis-makes-its-blood-sausage-1683769387.
10. I. Bodolan, *Impactul noilor tehnologii asupra procesului de intelligence*, 7 November 2012, available at http://intelligence.sri.ro/impactul-noilor-tehnologii-asupra-procesului-de-intelligence/.
11. A. De Borchgrav, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, CSIS Homeland Defense Project, CSIS Press, Washington, D.C.,2001.
12. N. Bradley, *Cyberterrorism Is Real – Is It?*, Twickelerveld Intelligence and Investigations, available at http://www.intelligence-and-investigations.com/media/uploads/62_Cyberterrorism%20-%20Nicholas%20Bradley.pdf.
13. N. Briggs, *Conflict Diamonds in West Africa*, 5 December 2003, available at https://web.stanford.edu/class/e297a/Conflict%20diamonds%20in%20West%20Africa.htm.

14. F. Casota, *Între carul cu boi şi agricultura 4.0*, 17 March 2017, available at http://www.businessmagazin.ro/cover-story/intre-carul-cu-boi-si-agricultura-4-0-16190499.
15. I. Chifu, *Arme mai puternice decât cele nucleare devin operaționale: primul laser funcțional montat pe un vas american*, în *Pulsul planetei*, 2017, available at https://evz.ro/arme-mai-puternice-decat-cele-nucleare.html.
16. B. Collin, *The Future of Cyber Terrorism*, Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996.
17. D. Cristea, *Rolul tehnologiilor informatice şi de comunicații în desfăşurarea revoltelor din Primăvara Arabă*, în *Revista Comunicațiilor şi Informaticii*, nr. 1, 2012.
18. D. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, in J. Arquillaand D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Military*, Rand, Santa Monica, available at http://www.nautilus.org/info-policy/workshop/papers/denning.html.
19. James F. Dunnigan, *Noua amenințare mondială – Cyber-terorismul*, Editura Curtea Veche, Bucureşti, 2010.
20. M. Eggan, *Flash Crash: Could It Happen Again?,* 6 May 2014, available at http://money.cnn.com/2014/05/06/investing/flash-crash-anniversary/index.html.
21. P. Foster, *Bogus' AP Tweet about Explosion at the White House Wipes Billions off US Markets*, 23 April 2013, available at http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.
22. V. Fyndlay, *Research Study. Cyber-Threats, Terrorism and the Counter-Terror Model*, University of St. Andrew's, The Handa Centre for the Study of Terrorism and Political Violence, 2014, available at https://www.academia.edu/25263269/Cyber-Threats_Terrorism_and_the_Counter-Terror_Model_by_Valarie_Findlay_Cyber-Threats_Terrorism_and_the_Counter-Terror_Model.
23. M. Gorge, *Cyberterrorism: Hype or Reality?*, Computer Fraud & Security, 9-12, 2007, available at https://www.researchgate.net/publication/223089895_Cyberterrorism_hype_or_reality.
24. I. Grosu, *Serviciile de informații: Reformă sau transformare*, 26 July 2009, available at https://intelligence.sri.ro/serviciile-de-informatii-reforma-sau-transformare/.
25. M. Janakiram, *How IBM and Microsoft are Disrupting the Healthcare Industry with Cognitive Computing*, 3 January 2017, available at https://www.forbes.com/sites/janakirammsv/2017/01/03/how-ibm-and-microsoft-are-disrupting-the-healthcare-industry-with-cognitive-computing/#62c320a21a92.

26. J. Keller, *Military Intelligence Research Seeks to Uncover Threats from Social Media, other text*, available at https://www.militaryaerospace.com/articles/2015/08/military-intelligence-social-media.html.
27. J. Keller, *The Growing Role of Technology in the Global War on Terrorism*, 8 December 2015, available at http://www.militaryaerospace.com/articles/2015/12/counter-terrorism-technology.html.
28. J. Ling, *Man Who Sold F-35 Secrets to China Pleads Guilty*, 24 March 2016, available at https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.
29. E. Perez, *FBI: Hacker Claimed to Have Taken Over Flight's Engine Controls*, 25 May 2015, available at http://edition.cnn.com/2015/05/17/us/fbi-hacker-flightcomputer-systems /index.html
30. M. Tran, S. Khaw, *The man who founded Enron, Kenneth Lay, has died just weeks before his jail sentence was to be announced. Mark Tran and Stefanie Khaw look at one of America's biggest business scandals*, 6 July 2006, available at https://www.theguardian.com/business/2006/jul/06/corporatefraud.enron.
31. Z. Yunos, *Putting Cyberterrorism into Context. STAR In-Tech*, 2009, available at http://www.cybersecurity.my/data/content _files/13/526.pdf?.diff=1236049327.
32. https://ro.wikipedia.org/wiki/Darknet.
33. https://ro.wikipedia.org/wiki/Extragerea_de_cuno%C8%99tin%C8%9Be_din_date.

ROMANIAN MILITARY THINKING

romania2019.eu

THE WEAPONIZED NARRATIVE – THE NEW BATTLESPACE OF THE 21ST CENTURY

Captain BEng Viorica Ionela TRINCU

PhD candidate, "Carol I" National Defence University, Bucharest

In the geopolitical context of the 21st century, "the battle for hearts and minds" is ever more present. The advance of new technologies has changed the conventional battle space dramatically. Nowadays, the new battlespace is represented by the weaponized narrative. The weaponized narrative is increasingly affecting our lives in a smaller or greater way by using different tools, the most dangerous one being the use of artificial intelligence (AI). The aim of this article is to explain how the new battlespace determines our existence by exploring the impact of AI on human lives.

Keywords: weaponized narrative, artificial intelligence, cognitive dimension, fake news.

Introduction

The major changes in the global security environment that have occurred at the end of the past millennium continue to mark the beginning of the 21st century, characterised by substantial changes in the classical parameters of the analysis of the evolution of international security. The beginning of the 21st century has brought into the spotlight less anticipated mutations with different effects, from the individual to state and non-state actors level.

Thus, if during the Cold War, we could speak of certain symmetry in the relations between the two great political and military blocs, we are currently witnessing the emergency of multiple forms of asymmetry in contemporary conflicts, as a result of the differentiation between conventional warfare and new kinds of wars. The present appears as a true conglomerate of risks, opportunities, uncertainties and threats, which will be powered by rapid social, scientific, technological and environmental changes, intensified by the effects of information technology era and globalisation. The development of information technology has revolutionised the way in which nations, armies, organisations and people interact. The liaison between the operational land, air, maritime, space, cyber, electromagnetic and cognitive environments is represented by the information environment.

In a globalised world, wars are no longer waged, lost or won exclusively on the classic combat front, in the physical dimension, but can shift their centre of gravity, depending on the context, towards the information dimension with very high weight in the cognitive space – the space of alternative narratives.

In 2017, Professor Ion-Aurel Pop, Chairman of the Romanian Academy, said: *"Information and communication are of enormous importance for historical research. It was said, not a long time ago, that he who owns information owns the world. Today, something more is added – he who owns communication can rule the world or own wider communities. Much of the deformations that work in today's world have had theoretical bases in history. In order to be able to compare and respond to these challenges, we need to cultivate our most powerful computer, the human brain"*[1]. Thus, the 21st century

[1] Nicușor Ciobotea, *Războiul informațional, sub lupă, Conferință la Academia Română*, 26 April 2017, https://www.promptmedia.ro/2017/04/razboiul-informational-sub-lupa-conferinta-la-academia-romana/, retrieved in December 2018.

ROMANIAN MILITARY THINKING

has offered a new value to the battlespace due to the paradigm shift. In a globalised world, wars are no longer waged, lost or won exclusively on the classic combat front, in the physical dimension, but can shift their centre of gravity, depending on the context, towards the information dimension with very high weight in the cognitive space – *the space of alternative narratives*. Thus, the confrontations of modern states and armed forces are mainly transferred at the mental level, of the human psyche, and uses the most sophisticated instruments, such as artificial intelligence.

Culture allows us to resist lies and manipulation by offering strong support points, which can hardly be dismantled. As the internal and external state systems change, due to transformations produced by globalisation, technological evolution and progress, the use of traditional narratives may prove inappropriate. Individuals can be perceived as beings in search of patterns of connection and socialisation, unable to tolerate the lack of meaning.

The weaponized narrative

Modern psychology and behavioural economics strengthen theories in the fields of social sciences and journalism, according to which human attitudes and behaviours are directed by narratives. Narratives, often implicit, represent the nucleus of human identity. Narratives provide the ideal environment for the development of individuals and social groups in traditionalist societies based on well-founded and rooted cultural norms. Culture allows us to resist lies and manipulation by offering strong support points, which can hardly be dismantled[2]. As the internal and external state systems change, due to transformations produced by globalisation, technological evolution and progress, the use of traditional narratives may prove inappropriate. Individuals can be perceived as beings in search of patterns of connection and socialisation, unable to tolerate the lack of meaning. People need myths, and the narrative is essential to what it means to be human[3].

In such circumstances, in which the great challenge to human existence and identity stems from the effects of modernity, individuals tend to adopt the new narratives, especially the simple and understandable ones. Moreover, because the effects of modernity will gradually change human civilisation, individuals tend to protect and return to traditional narratives, for fear of not losing their human identity. In this way, they see as enemies those who do not share their visions. It is, in other words, about manipulation, if we accept the explanation according to which *"to manipulate means first of all to build an image of reality which seems to be"*[4].

Once a defensive narrative is adopted, it tends to become stronger, especially when it depends on certain facts. For example, in some respects, poverty and corruption in Russia strengthen, and not undermine, the narratives relating to national identity and power. This type of narrative is spread by the national media, being less critical to the national identity. This conservative nationalism arises in response to the effects of modernity and is entirely predictable, although it can take particular forms, depending on each society.

The *weaponized narrative* is a relatively new concept, being part of a project launched by the Center on the Future of War of Arizona State University, USA[5].

Weaponized narrative is a set of techniques and means that rely on the use of disinformation, fake news, information technology and artificial intelligence, with the aim of destroying or undermining the human identity, society and civilisation of the opponent, by creating a state of confusion and social disunion.

So how can the *weaponized narrative* be defined? It is a set of techniques and means that rely on the use of disinformation, fake news, information technology and artificial intelligence, with the aim of destroying or undermining the human identity, society and civilisation of the opponent, by creating a state of confusion and social disunion[6]. This is a general definition, as the current stage of human development, the one of the rapid evolution of technology, as well as the stage of geopolitical, geo-economics and cultural tendencies that contribute to the exacerbation of the weaponized narrative strengthen the statements according to which human civilisation is not at the end of an historical era, but at its beginning, and any claim of certainty would be simply premature.

What can now be seen is that the weaponized narrative attacks both the faith and the common cultural values of the opponent, representing an emerging field of the hybrid war. This is based on methods specific to disinformation, propaganda, information warfare, psychological warfare, taking into account progress in areas such as evolutionary psychology, behavioural economics, cognitive sciences, modern marketing and media studies and artificial intelligence.

The weaponized narrative takes place at all levels: tactical, operational and strategic. *At tactical level*, the main objective

[2] *Weaponized Narrative: The New Battlespace, Center on the Future of War*, March 2017, https://weaponizednarrative.asu.edu/file/272/download?token=kV886rEe, retrieved in January 2019.

[3] *Ibid*.

[4] Philippe Breton, *Manipularea cuvântului*, Editura Institutului European, Iași, 2005, p. 18.

[5] *Weaponized Narrative: The New Battlespace, Center on the Future of War*, March 2017, https://weaponizednarrative.asu.edu/file/272/download?token=kV886rEe, retrieved in March 2019.

[6] Mihail Orzeață, *The War Humanity Has Always Waged against Itself,* Armed Forces Academy of General Milan Rastislav Štefánik, *Liptovský* Mikuláš, Slovak Republic, 2012, pp. 188-189.

ROMANIAN MILITARY THINKING

of the weaponized narrative is the weakening of potential opponents, avoiding the specific means of conventional warfare. Such an example is represented by the invasion of the Russian Federation in the Crimea Peninsula.

The specific initiatives are represented by the way in which the weaponized narrative is carried *at operational level*. This type of strategy is mainly specific to asymmetric confrontations, in which state and non-state actors are incapable of competing on the international scene using conventional means.

At strategic level, the weaponized narrative uses means to destabilise opponents in time, neutralising their ability to interfere with the plans and interests of the attacker, with an impact in achieving the objectives set. The intervention of the Russian Federation in the American and European presidential elections, in a continuous effort to weaken and divide the West, is an edifying example of the use of techniques specific to the weaponized narrative at strategic level.

An example of using the narrative with a strategic purpose, in the past, with means and techniques based on different social, cultural and ethnic instruments is that of the long-term subordination of the Baltic States by the Russian Federation before the Second World War. In a first phase, in December 1939, data was collected on the political leaders considered to be hostile towards Moscow, then an extremely aggressive campaign was launched in the press, aiming to diminish pro-Western sympathies. Then followed the ultimatums in June 1940, and the Baltic States, abandoned ever since August 1939, through the Ribbentrop-Molotov Pact, were forced to accept them. In August 1940, all three Baltic States – Lithuania, Latvia and Estonia – became part of the Soviet Union.

The intense information flow is the ideal environment for conducting this kind of battle. Such an attack provides the target opponent with reduced time to process and evaluate the situation, being enough disoriented at cognitive level to analyse the state in which he is. In such situations, there are many opportunities for emotional manipulation that undermine the opponent's willingness to resist.

Artificial intelligence and information technology – vehicles of weaponized narrative

The intense information flow is the ideal environment for conducting this kind of battle. Such an attack provides the target opponent with reduced time to process and evaluate the situation, being enough disoriented at cognitive level to analyse the state in which he is. In such situations, there are many opportunities for emotional manipulation that undermine the opponent's willingness to resist.

romania2019.eu

The simple question "*Is this information real?"* could, in most cases, represent a significant improvement in terms of finding the truth. American General Stanley A. McChrystal said "*to defeat a network you need another network*"[7]. Propagandists use networks (socially manufactured, such as *botnets*[8]) to spread confusion and disinformation among the population. Recent advances in the field of cognitive sciences have highlighted the vulnerabilities of human societies to the negative effects of disinformation.

When fake news is sent to someone's social *feed*[9], even a single individual who says "*Maybe this information is not true*" can lead to increased probability of finding the truth. Of course, this process is a difficult one, involving a very long time. Information that is based on pre-existing views is easier to accept. However, if human individuals had a thorough understanding of the importance of finding the truth, then the likelihood of questioning different information would increase significantly. If enough individuals find the motivation required to ask questions, then questions can uncover the truth.

Narratives have enough power to maintain the target audiences involved in this kind of battle, as long as the behaviour of central actors is consistent with the expectations.

Over the next decade, a wide range of actors will develop and install systems that are based on manipulation, with very few restrictions in terms of widespread use. Governments have a slow response to threats, due to ignorance or concerns about restricting the freedom of expression. Consequently, we can say that, in some cases, the nations themselves fuel the narratives that exacerbate social discord and undermine the belief of the population in their own governments.

Each battle is unique and, therefore, a combination of methods and techniques is used, including "*troll farms*"[10], which exacerbate

Over the next decade, a wide range of actors will develop and install systems that are based on manipulation, with very few restrictions in terms of widespread use. Governments have a slow response to threats, due to ignorance or concerns about restricting the freedom of expression. Consequently, we can say that, in some cases, the nations themselves fuel the narratives that exacerbate social discord and undermine the belief of the population in their own governments.

[7] *Weaponized Narrative: The New Battlespace, Center on the Future of War*, March 2017, https://weaponizednarrative.asu.edu/file/272/download?token=kV886rEe, retrieved in January 2019.

[8] A botnet is a string of connected computers coordinated together to perform a task. Botnets gain access to a machine through some piece of malicious coding, then contact the master computer to let it know that the machine is entirely under the control of the cyber attacker and it can carry out other nefarious tasks. Independent computers are known as *bots* or *zombies*, according to https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

[9] A *feed* is a stream of content that you can scroll through. The content appears in similar-looking blocks that repeat one after the other. See https://support.google.com/adsense/answer/9189559?hl=en-GB.

[10] A troll farm is an organisation whose employees or members attempt to create conflict and disruption in an online community by posting deliberately inflammatory or provocative comments. See https://www.collinsdictionary.com/us/submission/17707/troll+farm.

ROMANIAN MILITARY THINKING

social, racial and ethnic tensions in target societies, through stealing documents and personal data to influence elections or to develop campaigns aimed at weakening population confidence in state institutions. In this context, the weaponized narrative uses the new methods and means of technology to create and maintain the necessary prerequisites for the outbreak and development of such confrontation. Such a method is given by the use of Artificial intelligence (AI), which is an evolutionary collection of technologies that enables computers to simulate cognitive processes similar to the elements of human thinking[11]. The current instruments and technologies underlying artificial intelligence are limited to specific tasks, such as providing driving directions or recognising faces in images, which are not instruments of general intelligence applicable in many areas. Sensorial super-intelligent systems that go beyond human skills are still "work in progress", but IA technology is already successfully used in various robotic industries or in the development software and still belong to science fiction are not taken into account.

However, the next wave of AI technologies will probably produce a new contextual adaptation in which systems build explanatory models for the classes of real world phenomena. These models will increase the ability of the AI systems to reason and summarise, which would lead to the transition from natural language processing to its understanding.

However, the next wave of AI technologies will probably produce a new contextual adaptation in which systems build explanatory models for the classes of real world phenomena[12]. These models will increase the ability of the AI systems to reason and summarise, which would lead to the transition from natural language processing to its understanding[13]. In this new context, AI systems will be able to understand the significance of text, communication and reason, in other words, capabilities increasingly linked to human understanding. Understanding human language and its related technologies leads to the emergence of machines that have the ability to communicate in a manner similar to that of human individuals.

The automated learning process, known as *machine learning*, underpins the development of AI systems. It consists in the extraction of unlabelled data (unattended learning) or the efficient categorisation

[11] Matt Chessen, *The Madcom Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy... and What Can Be Done about It*, Atlantic Council, 2017, p. 6, https://issuu.com/atlanticcouncil/docs/the_madcom_future_rw_0926, retrieved in December 2018.

[12] John Launchbury, *A DARPA Perspective on Artificial Intelligence*, YouTube Video, 16:11, DARPAtv, 15 February 2017, https://www.youtube.com/watch?v=-O01G3tSYpU, retrieved in December 2018.

[13] Venkat Srinivasan, *Context, Language, and Reasoning in AI: Three Key Challenges*, in *MIT Technology Review*, 14 October 2016, https://www.technologyreview.com/s/602658/context-language-and-reasoning-in-ai-three-key-challenges/, retrieved in December 2018.

of data based on pre-existing definitions embedded in a labelled dataset (supervised learning)[14]. In simple language, machine learning enables computers to act and learn without being explicitly programmed. Developers provide machine learning systems that involve large amounts of data, with a view to finding possible information connections, to improve performance automatically.

romania2019.eu

Machine learning is a method used in the Google search algorithm, digital advertising, and online personalisation tools (Amazon and Netflix referral engines or Facebook newsfeed). It also extends to quantitative processes, such as supply chain operations, financial analysis, product prices and public procurement forecasts. Almost every industry explores or uses automatic learning applications.

Deep learning uses additional hierarchical processing layers similar to neural structures in the brain and large datasets to shape high-level abstract elements in order to recognise highly complex data models[15].

Big data[16], combined with automatic learning tools, will increase the ability of the AI systems to influence individuals through personalised propaganda. The Cambridge Analytica Company argued, in 2016, that it had between three and five thousand databases per individual and the psychological profiles of 230 million adults in the US[17].

Big data, combined with automatic learning tools, will increase the ability of the AI systems to influence individuals through personalised propaganda. The Cambridge Analytica Company argued, in 2016, that it had between three and five thousand databases per individual and the psychological profiles of 230 million adults in the US.

The exponential development of concepts such as Internet of Things and the spreading of interconnected devices, such as smart watches, retail store sensors and dozens of other gadgets, result in the proportionate increase in the amount of data that will capture information about people's lives. Virtual Reality offers the possibility to test people's present reactions to hypothetical stimuli and to measure their responses to products and ideas subtlety introduced in the context of virtual experiences. Data Patents from private companies and government databases have exposed private information about their users and associates. More and more, users offer the most

[14] Matt Chessen, *op. cit.*, p. 7.

[15] John Launchbury, *A DARPA Perspective on Artificial Intelligence*, YouTube Video, 16:11, DARPAtv, 15 February 2017, https://www.youtube.com/watch?v=-O01G3tSYpU, retrieved in January 2019.

[16] Big data means too large and complex data sets that require new forms of processing in order to enable decision-making, discover significances and optimising processes, according to https://todaysoftmag.ro/article/879/big-data-si-social-media-marea-schimbare.

[17] Tom Cheshire, *Behind the Scenes at Donald Trump's UK Digital War Room*, *Sky News*, 22 October 2016, http://news.sky.com/story/behind-the-scenes-at-donald-trumps-uk-digital-war-room-10626155, retrieved in December 2018.

intimate details online, expressing their views or posting photos from family vacations.

Data proliferation facilitates total exposure of the individual, from personality to political orientation. A study was able to determine the sexual orientation, ethnicity, religious and political affiliation, personality traits, intelligence, state of happiness, use of addictive substances, parental separation, age and gender of Facebook users depending on the number of *"likes"*. Thus, it has been found that machines can determine users' personalities better than collaborators, friends or family members can do. Many aspects of personality and behaviour can be accurately predicted without human analysis, simply by using data.

The human cognitive system is a complex one, and machine learning tools are very well developed, therefore it is very likely that they could decode complex systems. Communication generated by the AI systems will not be the mass media, but will be customised to communicate data on the political affiliation of an individual, their vision of the world, as well as the psychological needs and vulnerabilities.

The human cognitive system is a complex one, and machine learning tools are very well developed, therefore it is very likely that they could decode complex systems. Communication generated by the AI systems will not be the mass media, but will be customised to communicate data on the political affiliation of an individual, their vision of the world, as well as the psychological needs and vulnerabilities.

The access to these technologies is not limited to corporations or state-sponsored actors. AI tools are widely available (Google Tensor Flow, Microsoft control Tool and many other AI tools are free and open source) and can operate on any regular computer.

A predictable future?

It has become obvious that, no matter the scenario we relate to, AI-based technologies will deeply influence the future of human civilisation.

Social media interactions, internet surfing and even shopping provide thousands of pieces of information from which technologies can build psychological profiles for almost every user. Providing personal information leads to the creation of databases necessary for machines in order to have a better knowledge of our personalities, desires, needs, inconveniences and fears, most of the time, even better than we know them ourselves.

The advance in the field of artificial intelligence will soon enable extremely persuasive and manipulative communications generated by machines. In these circumstances, an automated system using online data and easily accessible marketing databases can determine

personalities, political preferences, religious affiliation, demographic data and personal interests. By knowing the news sites and social media platforms that users visit, the system dynamically creates content – everything from comments to complete articles –, a concept designed specifically to connect to the psychological framework of users, with the purpose of obtaining a specific result. This content could be a collection of real facts, lies or a combination of truth and lie, sufficient to achieve the desired effect.

The AI system will be able to detect human emotions at least the same or even better than people can. Similarly, it will convincingly imitate the human emotion that resonates with the personality and emotional state of any human being. Moreover, it will be able to synthesise a pliable reality in real time, in response to emerging events. It will accurately modify the video and audio content of politicians to make users say and do things that support their narrative, and will generate news articles and videos about events that never happened in order to shape public perception.

The AI system will be able to detect human emotions at least the same or even better than people can. Similarly, it will convincingly imitate the human emotion that resonates with the personality and emotional state of any human being. Moreover, it will be able to synthesise a pliable reality in real time, in response to emerging events.

The threshold of profitability in the case of IA systems multiplication will be maximal. Similar to other digital tools, once this AI system is created and configured, the marginal cost of creating multiple such systems will be almost zero. So there could be millions of AI manipulation bots surfing the Internet, twenty-four hours a day, seven days a week, transmitting certain messages to change human behaviours. The online information environment will be overwhelmed by a speech oriented towards the man-machine interaction, intended to sell, persuade, intimidate, distract, sustain, inform, misinform and manipulate.

Through enormous investment in the AI development, technological evolution is expected to completely change the whole world.

Large companies such as Google, IBM and Amazon, make significant progress in the development of the AI, bringing on the international stage a race of technologisation between non-state actors, similar to the US and USSR arms race in the Cold War era. No one and nothing can guarantee, at this time, the safety of these automated machines, nor the fact that they will be used strictly for a noble purpose and not in the interests of those who want to affect the proper conduct of human activities and security. Technology enthusiasts exhibit an acutely eager anticipation for the time when technologised assemblies will reach

ROMANIAN MILITARY THINKING

the anticipated potential, but those whose activity is to maintain the security of citizens and the systems serving them are rather concerned with the ethical and legal principles that will lie at the basis of the operation and use of artificial intelligence.

In a scientific seminar, organised on the occasion of the opening of the new school year, Vladimir Putin discussed with students about the advantages of the information age, stating that "*the future belongs to artificial intelligence*" and whoever leads in AI will rule the world: "*Artificial Intelligence is the future, not only for Russia, but for all mankind. It comes with colossal opportunities, but also threats difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world*"[18].

At the institutional level, the creation of a well-regulated and easy-to-check environment remains the only solution for the proper functioning of the AI-based systems, thus reducing errors that may diminish the advantages of technological developments.

Conclusions

The implications of an information environment *"contaminated"* by weaponized narratives for military and security organisations engaged in democratic states or for Romania as a whole are not entirely clear. However, one must find the means and methods necessary for countering the harmful effects generated by these weaponized narratives. Under the scope of the new unconventional attacks, companies and institutions must adapt to the challenges presented by these new threats.

At the institutional level, the creation of a well-regulated and easy-to-check environment remains the only solution for the proper functioning of the AI-based systems, thus reducing errors that may diminish the advantages of technological developments, while at the individual level, we must insist that there is a truth, an objective reality, and that it is our duty as individuals to find and focus on this truth.

BIBLIOGRAPHY

1. ***, *Weaponized Narrative: The New Battlespace*, Center on the Future of War, March 2017, https://weaponizednarrative.asu.edu/file/272/download?token=kV886rEe.
2. ***, *Weaponized Narrative Initiative*, Arizona State University, 2017, https://weaponizednarrative.asu.edu/.
3. ***, *Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day*, RT, 1 September 2017, https://www.rt.com/news/401731-ai-ule-world-putin/.
4. 4. B. Allenby, J. Garreau, *Weaponized Narrative is the New Battlespace*, *Defense One*, http://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/?oref=defenseone_today_nl.
5. Tom Cheshire, *Behind the Scenes at Donald Trump's UK Digital War Room*, *Sky News*, 22 October 2016, http://news.sky.com/story/behind-the-scenes-at-donald -trumps-uk-digital-war-room-10626155.
6. Matt Chessen, *The Madcom Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy... and What Can Be Done about It*, Atlantic Council, 2017, https://issuu.com/atlanticcouncil/docs/the_madcom_future_rw_0926.
7. Nicușor Ciobotea, *Războiul informațional, sub lupă, Conferință la Academia Română*, 26 April 2017, https://www.promptmedia.ro/2017/04/razboiul-informational-sub-lupa-conferinta-la-academia-romana/.
8. John Launchbury, *A DARPA Perspective on Artificial Intelligence*, YouTube Video, 16:11, DARPAtv, 15 February 2017, https://www.youtube.com/watch?v=-O01G3tSYpU.
9. Stanley A. McChrystal, *It Takes a Network: The New Front Line of Modern Warfare,* in *Foreign Policy*, March/April 2011, http://foreignpolicy.com/2011/02/21/it-takes-a-network/.
10. Venkat Srinivasan, *Context, Language, and Reasoning in AI: Three Key Challenges*, in *MIT Technology Review*, 14 October 2016, https://www.technologyreview.com/s/602658/context-language-and-reasoning-in-ai-three-key-challenges/.
11. Ryan Whitwam, *Google's Deep Mind Develops Creepy, Ultra-Realistic Human Speech Synthesis*, Geek.com, 9 September 2016, www.geek.com/tech/googles-deepmind-develops-creepy-ultra-realistic-human-speech-synthesis-1670362/

[18] *"Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day", RT*, 1 September 2017, https://www.rt.com/news/401731-ai-rule-world-putin/, retrieved in January 2019.

ROMANIAN ARMED FORCES – PUBLIC SERVICE

Brigadier General Corneliu POSTU
Director of the Defence Staff

Since ancient times, within nation-states, organised in different forms of social systems, there have functioned both civilian (healthcare, education, justice etc.) and military institutions, meant to defend national integrity against external threats. Throughout time, in the event of evident and extreme threats, the two components – civilian and military – have cooperated to ensure and protect the welfare of the society.

Being in a permanent connection with the society, whose component part they are, the armed forces establish with the society relations defined by a series of characteristics such as: variety, legality, complexity and interdependence. Thus, the armed forces assume not only the role of "guardian of the City" but also that of public service, an entity in the service of the society.

Considering the complexity of hypotheses, their veracity has been scientifically proved by using interdisciplinary research methodologies, in order to thoroughly explain the phenomenon, as well as by analysing and synthesising the data collected from relevant bibliographical sources, allowing for providing new and original points of view with arguments.

Keywords: public service, civil-military relations, legality, complexity, interdependence.

English version by **Diana Cristiana LUPU**.

Introduction

The role and place of the military within the society have aroused, throughout history, constant interest for the general public, materialised in studies and research projects conducted in several academic disciplines, such as political philosophy, sociology, political science or security studies.

In the dialogues in *The Republic*[1], Socrates considers necessary an army consisting of professionals. Glaucon, being accustomed to the citizen-soldier of Athens, expresses his bewilderment. Socrates argues that his vision is a consequence of *oikeiopragia*[2]: as the shoemaker should be a shoemaker and nothing more, the soldier should be the *"guardian of the City"*, in Plato's terms, and nothing more. However, is the situation of the *"guardian"* equivalent to that of the carpenter, the farmer or the doctor? Socrates argues that it is true, given that what generates the best results in the case of ordinary trades should also lead to the same positive results in the particular case of the guardians.

Is Plato's vision of the role of the military-guardian still relevant in the current society? In Romania, and not only, the transition to a democratic society and the processes entailed by the membership of NATO and the EU have led, during the past three decades, to the necessity of establishing democratic civil-military relations. In order to meet the mentioned goal, the following theoretical aspects have been considered: civil-military relations, civilian democratic control, military professionals and civil-military cooperation (CIMIC)[3].

It is evident that civil-military relations are the relations established between the civilian and military components of the society. To define

In Romania, and not only, the transition to a democratic society and the processes entailed by the membership of NATO and the EU have led, during the past three decades, to the necessity of establishing democratic civil-military relations.

[1] See https://kupdf.net/queue/146045751-republica-lui-platon_590ecae9dc0d60c11c959e8d_pdf?queue_id=-1&x=1564123633&z=MjEzLjE3Ny40LjE1MA==, p. 17, retrieved on 15.07.2019.

[2] Term used by Plato, in *The Republic*, to demonstrate the fact that the products of labour are better, more numerous and more rapidly manufactured when each individual does what it is appropriate, each of them minding its own business in the city. Plato later calls such behaviour *oikeiopragia*. It is the idea the *Republic* is built upon.

[3] Marian Zulean, *Militarul și societatea. Relațiile civil-militare la începutul mileniului al III-lea*, Editura Militară, București, 2008, p. 15.

the terms *civil* and *military* in the context of the society, Daniel Nelson[4] suggests a matrix having two inputs, within which the two components are defined in general and in particular (figure no. 1). Thus, according to Daniel Nelson, the term *military* is defined, in the narrow sense, as the armed forces military personnel, and, in the broad sense, as any type of personnel within any national social structure. The term *civil* is defined, in the narrow sense, as a political decision-maker, and, in the broad sense, as the entire society. Based on these interpretations, Nelson understands the relationship between the two components in a dynamic key, characterised by both conflicting and cooperative interactions.

According to Daniel Nelson, the term military is defined, in the narrow sense, as the armed forces military personnel, and, in the broad sense, as any type of personnel within any national social structure. The term civil is defined, in the narrow sense, as a political decision-maker, and, in the broad sense, as the entire society.

Military / Civil	**Narrow definition** Armed forces, especially professional military personnel	**Broad definition** All national security institutions plus associated groups
Narrow definition Government institutions and occupants of the posts	I. The military personnel and the political elite interact without regard to the democratic process and public opinion. (Huntington)	II. Security structures interact with the political elite through pacts.
Broad definition The public sphere, civil society and mass media included	III. The political sphere and the civil society interact with the military personnel – potential tense relations.	IV. Security structures interact with the public based on a dialogue on the nation threats and capability.

Figure 1: Definition of the civil and military components of the society[5]

The concept of *democratic control* practically represents the central pillar of the civil-military relations theory and it refers to the civilian authorities, democratically elected, exercising control over the armed forces[6].

[4] Daniel N. Nelson, *Definition, Diagnosis, Therapy – A Civil-Military Critique*, Defense&Security Analysis, vol. 18, 2002, no. 2, pp. 157-170.

[5] Marian Zulean, *op. cit.,* p. 17.

[6] See Andrei Vocilă, *Dinamica fenomenului militar românesc după 1990 în relație cu factorul politic și social*, https://andreivocila.wordpress.com/2010/11/08/dinamica-fenomenului-militar-romanesc-militar-romanesc-dupa-1990-in-relatie-cu-factorul-politic-si-social/, retrieved on 10 June 2019.

The relevance and necessity of exercising democratic control over the security sector represent important issues in the Euro-Atlantic area. In this respect, the predecessor of the current OSCE, namely former Conference for Security and Cooperation in Europe, developed a *Code of Conduct on Politico-Military Aspects of Security*, adopted in Budapest, in 1994[7]. The mechanism of democratic control over the armed forces includes three basic provisions as follows:

1. the main normative assumption is that the military personnel should not be directly involved in domestic policy and that they should remain apolitical public servants of the democratically elected government;

2. the design and development of the defence policy should be conducted under the control of civilian authorities, the military personnel having the responsibility to implement the adopted decisions;

3. the decision to employ armed forces in the event of crises, internal or external, should be taken following the civilian authorities order[8].

Therefore, the democratic control over the security sector is *"the privilege of an institutional system, mainly sanctioned at institutional level as well as by normative acts having a lower level than the Constitution, in which mainly participates the legislative power, beneficiary of democratic legitimacy; its participation is both direct and indirect, being also added the executive power (bi-cephalous in our country, consisting of both the Government and the President), the judicial power, as well as other specially designed bodies"[9].* Concretely, the exercise of Parliamentary control in Romania has available the following mechanisms: questions, interpellations, simple motions, motions of no confidence, parliamentary debates[10].

The concept of democratic control practically represents the central pillar of the civil-military relations theory and it refers to the civilian authorities, democratically elected, exercising control over the armed forces.

[7] *Budapest Summit Declaration*, CSCE, *Budapest Document 1994, Towards a Genuine Partnership in a New Era*, see www.osce.org/mc/39554?download=true, retrieved on 10 June 2019.

[8] Marian Zulean, *op. cit.*, p. 19.

[9] George-Dorinel Dumitru, Dragoş-Adrian Bantaş, *Controlul democratic asupra sectorului de securitate – privire comparativă asupra modelului european şi aplicării acestuia în România*, in *Gândirea Militară Românească*, 1st ed.-2/2018, published by the Defence Staff, Bucureşti, pp. 184-185.

[10] See the *Regulations on the Chamber of Deputies*, adopted by the Decision of the Chamber of Deputies no. 8/1994, synthesis – 10 June 2019, cap. IV, p. 28, http://www.cdep.ro/pdfs/tab_acte/Regulament-din-1994-forma-sintetica-pentru-data-2019-06-10.pdf, retrieved on 7 July 2019.

ROMANIAN MILITARY THINKING

As far as military professionalism is concerned, Samuel P. Huntington, one of the founders of civil-military relations theory, considers that it is characterised by three attributes that are specific to the profession understood as vocation, namely expertise, responsibility and corporatism[11]. Expertise is understood as the quality of a person who has particular knowledge and skills specific to the performance of a certain job. The professional officer can put into practice his/her specific expertise (knowledge and skills) regardless of place and time, on behalf of the entire society, which translates into responsibility. Corporatism in the military profession refers to the esprit de corps, the camaraderie, the uniqueness provided to the group by the specific abilities possessed by its members to accomplish their missions.

As far as military professionalism is concerned, Samuel P. Huntington, one of the founders of civil-military relations theory, considers that it is characterised by three attributes that are specific to the profession understood as vocation, namely expertise, responsibility and corporatism.

A relevant distinction between the armed forces professionalism, in general, and the democratic armed forces professionalism is found in Marybeth P. Ulrich, within the US War College, in the paper *Democratizing Communist Militaries*. Ulrich considers that professional armed forces will meet the requirements of the legitimate elected government, regardless of its political colour, by respecting the following conditions: correctly defined missions, provision of specific military expertise for any military action, clear rules on the armed forces responsibilities[12].

CIMIC or civil-military cooperation represents the modality through which the military cooperate with the civilians to successfully accomplish the mission. Briefly, CIMIC is a NATO doctrine intended for the creation of the favourable conditions so that the mission within an Allied operation could be accomplished. Moreover, the term is also used to describe the armed forces employment in humanitarian crisis situations.

[11] Samuel P. Huntington, *The Soldier and the State. The Theory and Politics of Civil-Military Relations*, The Belknap Press of Harvard University Press Cambridge, Massachusetts, London, 1957, pp. 8-9.

[12] Marybeth Peterson Ulrich, *Democratizing Communist Militaries: The Cases of the Czech and Russian Armed Forces*, Michigan, University of Michigan Press, 1999, pp. 108-112.

The Armed Forces and the Civil Society: Different Roles, Common Goal

romania2019.eu

In Romania, the fundamental law of the state presents the armed forces as being *"exclusively subordinate to the will of the people to guarantee the state sovereignty, independence and unity, the territorial integrity of the country, and the constitutional democracy"*[13]. Under the conditions of the fundamental law of the country and of the international treaties to which our country is party, within the military alliance systems, the armed forces contribute to collective defence and participate in peacekeeping or peacebuilding actions. The membership of the North Atlantic Treaty Organisation has provided Romania with the opportunity to validate its democratic and pro-Western vocation. Moreover, the membership of NATO, the EU and the Strategic Partnership with the United States of America are the main pillars of national security.

The defence policy entails meeting the national and security objectives, the commitments in the field of defence assumed internationally, by employing the political, diplomatic and military instruments mobilised by the Ministry of National Defence in this respect. Its goal is to provide the necessary decisions and to conduct the necessary actions to guarantee the sovereignty, independence, unity and territorial integrity of Romania.

Huntington concludes that "nations that develop a proper balance of military-society relations increase their chance of finding the right answers to operational problems".

Returning to Huntington, we find that he identifies two levels to which national security policy can be related, namely: an operational level and an institutional level. Thus, at the operational level, consideration is given to identifying and taking measures to ensure national security against either external or internal threats. At the institutional level, the identification and connection of the military-society relations are aimed at, in order to develop a system to maximise security, while respecting social values. Thus, Huntington concludes that *"nations that develop a proper balance of military-society relations increase their chance of finding the right answers to operational problems"*[14].

In Romania, the military is a state institution, which exceeds the mere status of a state instrument, due to the functions it has in society

[13] *Constitution of Romania*, Chapter V, Section 1, Article 118 – the Armed Forces, https://www.constitutia.ro/art-118-fortele-armate.htm, retrieved on 12 June 2019.

[14] Marian Zulean, *Armata şi societatea în tranziție*, Editura Tritonic, Bucureşti, 2003, p. 82.

and its quality of the nation military power. From the organisational perspective, the armed forces represent a form of social organisation, their members acting on the basis of the correlation between the institutionalised norms and the execution of roles. Moreover, it should be also mentioned that, according to the normative system, the Ministry of National Defence is one of the actors that provide public services in the field of public order.

In the literature, regardless of the elements that are considered for their definition, it is stated, without exception, that the armed forces guarantee and symbolise the unity of the country and its traditions. The relationship between the armed forces and the civil society is one of the factors that are necessary for ensuring national stability, the reciprocal influence and interaction between the military service and the society being focused on both connections and conditions.

Public services should not be confused with public authorities, public institutions, specialised structures or legal entities of public or private law that provide the particular public service, in the public power capacity.

Even if civil society is based on systems of values related to democracy and freedom, to fundamental human and community rights, public services should not be confused with public authorities, public institutions, specialised structures or legal entities of public or private law that provide the particular public service, in the public power capacity.

The armed forces, on the other hand, even they are not, *stricto senso*, part of the civil society, are in close connection with it, considered either from the perspective of their members, as a significant number of civilians work for the armed forces, or from the perspective of the members of the military personnel families, who, in turn, are part of the majority, the civil society – politically affiliated or not, active members or supporters of some structures that define the *"civil society"* phrase. In essence, the armed forces are part of the society.

The Notion of Public Service

The *public service* has an ideological dimension as well as a political one that partially present the developments of the notion throughout time. The state and its administrative-territorial divisions, as organised forms of coexistence and activity, guarantee the necessary conditions for the citizens to conduct economic, social, cultural, security and other activities, which results in certain public services being organised by the state only, while others being organised by the local communities

acknowledged by the state. The public services established by the state perform the tasks proper to the executive power and constitute the administrative public services.

The notion of *"service"* is rooted in the Latin word *"servitum"*, meaning *"slave".* Some derived phrases are *"do someone a service", "provide a service"* or *"offer your services as something"*, which evokes the notion of *"public utility"* or *"public service".* In this regard, the public service entails a public management activity.

The public services established by the state perform the tasks proper to the executive power and constitute the administrative public services.

According to *Macmillan Dictionary of English Language*, the notion of *"service"* is defined as: *"a system provided by a government or official organisation for the needs of the public; help that you give to someone, especially by using your skills, ability or knowledge; help and advice given to customers; a business or organisation that earns money by provided help, information or advice for the public"*[15].

Until the post-war period, the theory of public services has not been developed. However, since the 18th century the theory has made certain progress. Thus, Jean Louis Mestre presented, in 1776, an edict containing different expropriation acts, which resulted in the establishment of some *"services of general interest"*.

Until the post-war period, the theory of public services has not been developed. However, since the 18th century the theory has made certain progress. Thus, Jean Louis Mestre presented, in 1776, an edict containing different expropriation acts, which resulted in the establishment of some "services of general interest".

Considering the approaches to defining the public service domain as well as their importance and time span, certain countries should be mentioned as references:

- in France, the notion was used in the *Blanco Affair* (1873), without being thoroughly studied. Although the notion was defined and sanctioned, dogmatically and juridically, by Leon Duguit, the Bordeaux School, its mentioning in the Preamble of the Constitution in 1946 did not lead to its thorough study, the notion being highlighted in the 1955-1960 period.

Jacques Chevallier[16] considers the notion of public service as a social entity, composed of activities and structures dependent upon the public communities in the public sphere.

- in the French literature, the accepted definition was that of the aggregate of a public community activities having as goal to meet certain general interest needs;

[15] *Macmillan Dictionary*, online ed., https://www.macmillandictionary.com/dictionary/british/service_1, retrieved on 12 June 2019.

[16] J. Chevallier, *Le Service Public*, Presses Universitaires de France, Paris, 1994, pp. 3-6.

ROMANIAN MILITARY THINKING

- in Italy, the phrase *"public services"* sanctions the scope of the continuity or equality principle in the public service;
- in Spain, the place and importance of public services are found in both the doctrine and national legislation, where the public services are organised according to regions and *"independent communities"*;
- in Germany, it is applied a system of administrative laws under the supervision of a specialised administrative litigation system;
- in the Netherlands and the UK, the concept is almost inexistent, the system in the latter being based on the *"common law"*.

In the late 19th century, the notion was further explained, the following aspects being highlighted and considered in defining the concept[17]:

In the late 19th century, the notion was further explained, the following aspects being highlighted and considered in defining the concept: state changes, economic life, social problems and political reinstatement; the dimension of the administrative judges competences, while they became independent in relation to the administration.

- state changes, economic life, social problems and political reinstatement;
- the dimension of the administrative judges competences, while they became independent in relation to the administration.

In this context, the divergences of opinions regarding the definition of the concept intensified, taking into consideration the expansion of administrative law and administrative judges competences. In this regard, a series of decisions were taken. Among them, there can be mentioned the Blanco (1873), Terrier (1903), Feutry (1908) and Therand (1910) decisions.

In conclusion, it can be stated that the evolution of the notion of public service is controversial and complex, and conceptual spheres are diversified, which is especially acknowledged in the administrative law. However, it is difficult to understand and define.

Public Service – Definition, Types, Characteristics

Since the notion of public service started to be used, the society has intended to put the notion into practice in different spheres. The public services sector is thus a set of constantly changing networks, based on diversified activities and modes of administration, permanently influenced by the moment of their establishment and by the activity sector. In a broad sense, the public service highlights the legal nature of the body that provides it, which can be the state, a public person, a local authority or any other public institution.

In the interwar period, the definition underwent changes, following the distinction between *"general interest"* and *"particular interest"*, the main goal of a public service being the interest of those administered and not a particular benefit.

From the legal point of view, the notion was not legalised, being considered both an activity and a structure simultaneously.

In the Western doctrine, three definitions of the public service have been identified, as follows:

- the classical one – at the beginning of the 20th century, the public service was presented as an activity of general interest, conducted by a public person only;
- the interwar one – developed following the economic progress, public services becoming thus flexible, varied and operational;
- the current one – outlined in the late '80s, when, following the evolution of democracy, it was established that certain public services provided by private persons could not benefit from the prerogatives of the public power.

From the perspective of the activities that were aimed at, public services, throughout their evolution, have been related to the following domains:

- *old public services* – related to the activities of the state institutions and aimed at protecting communities, ensuring public order, respecting laws and norms, collecting taxes, protecting civilians, and ensuring the forms of social communication;
- *economic public services* – forming the state economic public sector (in the early 20th century);
- *social services* – represented by social assistance and hospitalisation, public health and housing;
- *socio-cultural services* – focused on preserving and protecting the cultural heritage, information, research, arts, artistic and cultural activities, sports, environment etc., provided not only at the state but also at local level[18].

romania2019.eu

The public services sector is thus a set of constantly changing networks, based on diversified activities and modes of administration, permanently influenced by the moment of their establishment and by the activity sector. In a broad sense, the public service highlights the legal nature of the body that provides it, which can be the state, a public person, a local authority or any other public institution.

[17] Jacqueline Morand-Deviller, *Cours de Droit administratif. Thèmes de réflexion. Commentaires d'arrêts avec corrigés*, VII-ème édition, Paris I, Sorbonne, p. 454.

[18] J. Chevallier, *op. cit.*, pp. 66-71.

ROMANIAN MILITARY THINKING

According to Professor Paul Negulescu, the *public service* is *"an administrative body established by the state, county or commune, having determined competency and power, funded by the general budget of the establishing public administration, to regularly and continually meet a general need that can be met only partially or intermittently by a private initiative"*[19]. According to another author[20], the public service is the essential element of the modern state organisation, including the activities related to meeting collective interests.

From the technical-juridical perspective, the public service has the following characteristics: it is regularly and continually functional; it meets certain public interests; it is not intended for material benefits; it can undergo changes. The legislation related to public services has been aimed at harmonising them with the community acquis and facilitating the free movement of services, by transposing European directives into national legislation.

From the technical-juridical perspective, the public service has the following characteristics: it is regularly and continually functional; it meets certain public interests; it is not intended for material benefits; it can undergo changes. The legislation related to public services has been aimed at harmonising them with the community acquis and facilitating the free movement of services, by transposing European directives into national legislation.

In the *Constitution of Romania*, public services are presented in Art. 31 (radio and television), Art. 120 (principle of de-concentration), Art. 122 (role of the County Council) and Art. 123 (role of the Prefect). Moreover, according to the provisions of Art. 2 Para. (1) letter m) in the *Law of Administrative Contentious no. 554/2004*, as subsequently amended and supplemented, the public service is the activity organised/authorised by a public authority to meet a legitimate public interest. To define the public service, it should be also considered the principle of separation and balance of power in the state, sanctioned in Art. 1 Para. (4) in the Constitution.

The analysis of the legislative framework highlights a sectoral regulation of public services, for some areas the notion of *"system"* being used, such as defence, public order and national security system, healthcare system, national social assistance system.

In the social-economic life, the service sector has been materialised through the diversification and amplification of the services determined by the social needs, the wants and demands of the society, in close connection with the society level of development.

[19] Paul Negulescu, *Tratat de drept administrativ*, Tipografiile Române Unite, București, 1925, p. 621.
[20] Marin Văraru, *Tratat de drept administrativ român*, Editura Librăriei Socec & Co., Bucureşti, 1928, p. 89.

romania2019.eu

The services of public interest have an immaterial form, they are intangible, they cannot be separated in time and space, they are variable from one benefit to another, they conduct an activity having a social specific, intended for the public, they are in a permanent juridical relationship and under the control of the administrative authority that establishes and organises the particular service. Moreover, they also provide goods or services for the benefit of the community. In general, they are subject to a juridical regime based on the principles of law and can work even if they are not cost effective.

The principles underlying the organisation and functioning of public services are: *the principle of effectiveness*, which establishes the relation between the effort made and the results obtained, *the principle of equity*, which derives from the principle of equality of citizens before the law, and *the principle of decentralisation and de-concentration of public services*, which consists in the public services organising, functioning, controlling and disbanding by the local public administration authorities.

The principles underlying the organisation and functioning of public services are: the principle of effectiveness, the principle of equity and the principle of decentralisation and de-concentration of public services.

In the literature, *public services* are classified as follows:

- *in terms of their nature*: administrative, industrial and commercial;
- *in terms of aim*: necessary to meet the citizens needs, public services that provide benefits for private persons directly, and services intended for the communities in their aggregate;
- *in terms of the relationships with private services*: monopolised public services, public administration services provided in parallel with authorised persons, public services provided by private persons, authorised under the control of a public administration authority;
- *in terms of the opportunity to delegate*: public services that cannot be delegated to other persons and public services that can be delegated to other persons;
- *in terms of social importance*: vital and facultative;
- *in terms of scope*: public services of national importance, local services of regional importance – county, city, town, commune[21].

21 In Antonie Iorgovan, *Tratat de drept administrativ*, vol. I, Editura Nemira, 1996, p. 83.

ROMANIAN MILITARY THINKING

The public service as a notion related to the administrative law refers to those activities of general interest coordinated by the government and available for all the citizens of a particular state. The most comprehensive ones, in terms of aim, are the collective public services, which are provided for the general benefit of the community (armed forces, police, courts etc.).

Typology of Armed Forces – Society Relations

The evolution of the society as a whole is naturally reflected in the evolution of the military body, on the principle of the response of a viable organism to the stimuli of the environment in which it functions.

The relations between the armed forces and the society have developed, throughout time, according to the defining features of the two entities, the size, quality and forms of manifestation of these relations depending on the reality of the considered historical moment. The evolution of the society as a whole is naturally reflected in the evolution of the military body, on the principle of the response of a viable organism to the stimuli of the environment in which it functions. Being in an obvious connection with the society, whose component they are, the armed forces establish with the society relations that are defined by a series of characteristics such as: variety, legality, complexity and interdependence[22]. The mentioned relations allow for the armed forces to quickly and continually adapt to the reality, and to conduct the constitutionally appointed missions.

Being in an obvious connection with the society, whose component they are, the armed forces establish with the society relations that are defined by a series of characteristics such as: variety, legality, complexity and interdependence.

It is evident that there is a variety of relations between the armed forces and the society that reflect the connection between the two entities, *"among the relations between the armed forces and the civil society being the cooperation relations; the communication relations; the knowledge relations; the indifference relations; the rejection relations and the influence relations"*[23]. Certainly, regardless of the type of relations – be they economic, juridical, cultural, authoritarian, scientific etc., all of them contribute to the reciprocal exchanges between the armed forces and the society. Thus, through the economic relations, there is highlighted the link between the armed forces and the society from the perspective of the resources that should be allocated so that the military body can achieve all the legally assigned tasks. Buildings, training ranges, combat assets, ammunition, fuel, financial and human resources etc., as well as an appropriate education and training programme are, in the aggregate, the main elements specific to the military institution. The society ensures the necessary resources, the investment being, practically, one destined for ensuring national defence, the armed forces role being that of using the resources effectively so that they can accomplish their mission.

romania2019.eu

Practically, the economic relations between the armed forces and the society reflect the nature of the reciprocal dependence between the two institutions. Thus, under the conditions of ensuring the necessary resources, the armed forces will regularly conduct their activities and they will succeed in accomplishing their mission, the mission on which the very existence of the society that provides the necessary resources depends. The resources also play an important psycho-social role in the equation, as the personnel morale largely depends on them. A high military personnel morale will ensure the political neutrality of the armed forces as a state institution, which will represent a barrier to promoting political clientelism.

Another important set of relations between the armed forces and the society have a juridical nature. They are meant for ensuring the institutionalisation of the armed forces-society relations, especially through the notion of military operational law. By the package of laws developed by the legislative body, namely the Parliament, the armed forces status and role in society are highlighted.

Another important set of relations between the armed forces and the society have a juridical nature. They are meant for ensuring the institutionalisation of the armed forces-society relations, especially through the notion of *military operational law*[24]. By the package of laws developed by the legislative body, namely the Parliament, the armed forces status and role in society are highlighted. Thus, although, in essence, *"military operational law is public law, it also has elements of civil and commercial private law because, in situations of peace and armed conflict, military structures enter into juridical relations with civil authorities, civil society and private persons, especially in terms of the property regime, the procurement and the contracts for supply of resources, the request and grant of compensation for the material and moral damages caused to the civilians etc."*[25].

[22] Petre Duțu, *Armata şi societatea în tranziție*, Editura Academiei de Înalte Studii Militare, București, 2002, pp. 32-35.

[23] Doina Talaşman, *Considerații privind raporturile dintre istorie şi sociologie, respectiv armată şi societate*, in *Armata română şi societatea civilă*, studies presented within the Scientific Papers Session on the occasion of Military Archives Day, 92 years since the establishment of the Centre for the Study and Preservation of Historical Military Archives and 145 years since the establishment of the Armed Forces Historical Service, coordinators: Colonel Marian Moşneagu, PhD, Colonel Petrişor Florea, PhD, Cornel Țucă, PhD, Editura Istros, Pitești, 2012, p. 46.

[24] Notion initially used in the US Armed Forces, and then spread to other states and security organisations, mentioned in *Operational Law Handbook*, The Judge Advocate General's Schools Charlottesville, Virginia, 2010.

[25] Major (mil. just.) Cristina Ştefan Nicolaie, *Dreptul afacerilor civile în operații militare* (summary), București, 2015, p. 13.

Moreover, it should be mentioned the tendency towards reorienting and reorganising the military public law at both national and international level, an eloquent example in this respect being the movement of criminal institutions within the International Military Court in Nüremberg to civilian courts such as the current International Criminal Court. It is a reality that will have evident implications for the civil-military relations.

A relevant category of relations is also represented by those having a cultural nature. The armed forces have provided the society, throughout time, with cultural products that are extremely valuable, in the field of fiction, painting, plastic arts etc. In 1917, 35 plastic artists were mobilised within the Great General Headquarters in Iaşi by General Constantin Prezan. He intended to establish the National Military Museum, an institution *"where all the works presenting the most important pages, including the moments of restraint as well as the efforts made to meet the national ideal, in the history of the war should be kept for the future"*[26]. The list of mobilised sculptors contained the following names: Ion Jalea, Oscar Han, Ştefan Dimitrescu, Dimitrie Mățăuanu, Corneliu Medrea, Gheorghe Stănescu, Alexandru Călinescu, Camil Ressu, Ion Theodorescu-Sion, Nicolae Dărăscu, Grigore Negoşanu, Alexis Macedonski, Aurel Băeşu, Dumitru Brăescu, Constantin Bacalu, Petre Troteanu, Gh. Ionescu-Doru, Traian Cornescu, Emilian Lăzărescu, Ignat Bednarik, Atanasie Constantinescu and others. Moreover, starting on 2 February 1917, it was published the daily journal *România*, a *"national defence agency"*[27]. The Director was Mihail Sadoveanu, and the Editor-in-Chief was Octavian Goga. Among the members of the Editorial Staff were the following writers: Petre Locusteanu, Ion Minulescu, George Ranetti, N.N. Beldiceanu, Mircea Rădulescu, Corneliu Moldoveanu, Radu D. Rosetti and others. As collaborators there were: Nicolae Iorga, Ion Agârbiceanu, Vasile Voiculescu, Barbu Ştefănescu-Delavrancea, Alexandru T. Stamatiad, Zaharia Bârsan, Vasile Militaru etc.

In 1917, 35 plastic artists were mobilised within the Great General Headquarters in Iaşi by General Constantin Prezan. He intended to establish the National Military Museum, an institution "where all the works presenting the most important pages, including the moments of restraint as well as the efforts made to meet the national ideal, in the history of the war should be kept for the future".

The model that inspired General Constantin Prezan in making the decision to mobilise plastic artists within the Great General

[26] Barbu Brezianu, *Gruparea Arta Română*, in *Studii de istoria artei*, Plastic Arts Series, vol. 11, no. 1, 1964, pp. 149-150.

[27] See http://enciclopediaromaniei.ro/wiki/Mihail_Sadoveanu, retrieved on 23 May 2019.

Headquarters was that of General Carol Davila, MD, who, during the War of Independence in 1877-1878, invited Nicolae Grigorescu, Carol Popp de Szathmari, Sava Henția and G.D. Mirea to accompany the troops as attached to the Great General Headquarters Ambulance Service. General Carol Davila idea was that the artists could execute on-site drawings to be subsequently used, in the studio, to create works of art reflecting the Romanian troops heroism or mirroring the dramas of the civilian population as well as the horrors of war[28].

In the Romanian armed forces campaign during the Second World War there were also Alexandru Ciucurencu, Leonid Bulencea, Traian Sfințescu, Ion Musceleanu, Dumitru Ghiață, Valentin Hoeflich, Alexandru Țipoia among the painters who were on the front, felt the gunpowder smell, and described the reality there in a special way[29].

The paintings of Ion Țarălungă, for example, who was among the Air Force personnel during the communist regime, represent a really valuable collection presenting not only combat scenes but also aspects of the training process, having subjects belonging to all three services. Nowadays, the Armed Forces Plastic Arts Studio, whose Director is Valentin Tănase, is the main ambassador of the Romanian Armed Forces in the field of graphical representations.

Therefore, cultural relations highlight the reciprocal links between the society and the military institution. Through the varied cultural activities organised at the level of not only military units but also garrisons, a cultural exchange between the armed forces and the society is ensured. Through the works created by military writers, plastic artists and others, the armed forces contribute to the development of national culture. Moreover, through the entire personnel, the armed forces represent an important *"consumer"* of the cultural products of the society to which they belong.

Cultural relations highlight the reciprocal links between the society and the military institution. Through the works created by military writers, plastic artists and others, the armed forces contribute to the development of national culture. Moreover, through the entire personnel, the armed forces represent an important "consumer" of the cultural products of the society to which they belong.

A significant role in the armed forces-society relations is played by scientific activities. The military academic environment consists of a solid and viable network of military academies that provide

[28] See https://www.viata-libera.ro/prima-pagina/118267-centenarul-marii-uniri-pictori-si-sculptori-in-primul-razboi-mondial, retrieved on 23 May 2019.

[29] See https://armed.mapn.ro/nicolae-grigorescu---pictor-de-razboi-2326-23, retrieved on 23 May 2019.

the military personnel with scientific knowledge in compliance with the armed forces needs. The level of studies is up to the level of doctoral degree, and the cooperation with civilian higher education institutions enhances the degree of interaction between the armed forces and the society. Besides the didactical activity, there are also conducted scientific research activities, through the own scientific institutions and centres, in areas of interest for the armed forces, in particular, and for the society, in general. It is a domain in which there is cooperation, which results in numerous scientific research projects developed by the military systems finding their applicability within the society and vice-versa.

Complexity is another relevant characteristic of the relations between the armed forces and the society. Firstly, the armed forces, as a fundamental element of the society, are in a relation of dependency on the society. Considering the resources that are necessary for the military system are provided by the society, the relations within this process are closely connected to the degree of economic development of the society.

Complexity is another relevant characteristic of the relations between the armed forces and the society. Firstly, the armed forces, as a fundamental element of the society, are in a relation of dependency on the society. Considering the resources that are necessary for the military system are provided by the society, the relations within this process are closely connected to the degree of economic development of the society. Moreover, it is the society that decides the public policies, the national defence and security policy included, and the armed forces have the role of implementing the society decision. In addition, despite the character of force it has in the society, the military institution is subject to the rigours of civilian control and remains neuter in the political game within the society.

Considering the interdependence of the military-society relations, it can be highlighted the exchange of *"products and services"* between the two entities. For example, even if the primary beneficiary of the military education system is the military body, the civil society, in turn, benefits from the expertise of the military, either in different stages of their active career or by reintegrating them into the field of labour after retirement. On the other hand, the armed forces take on specialists trained in the civilian education system, to cover specialties that are not found in the own education system, but without which the military system cannot function. This type of transfer contributes to increasing the society's confidence in the armed forces and in their ability to fulfil the constitutionally assigned role.

The Romanian Armed Forces – Public Service for the Benefit of the Entire Society

Currently, the Romanian Armed Forces surpassed the theory of the soldier-citizen system and of the *"armed nation"*, based on mass armed forces, in which conscription led to the militarisation of the society. The emergence of the notion of *professional military personnel* has inevitably resulted in weakening the armed forces-society relation, especially *"with regard to certain issues such as the role of patriotism, of discipline in education, the goals of foreign policy, the image of the military profession"*[30]. On the other hand, an acute need for cooperation arises, considering that *"some of the logistic tasks and domains that do not have an immediate combat function are increasingly transferred to civilians and even to private companies"*[31].

In Romania, the Ministry of National Defence participates in the actions meant to eliminate the consequences of civilian emergencies through interagency coordination and cooperation, in compliance with the legal framework[32] that regulates the specific behaviour in such situations.

The Ministry of National Defence capabilities are employed to act in emergency situations, in compliance with the existing cooperation plans at central and local level, and the support functions established by the legislation in force. The main missions executed in this context are search and rescue, the participation in interventions in the event of emergency situations.

The Ministry of National Defence capabilities are employed to act in emergency situations, in compliance with the existing cooperation plans at central and local level, and the support functions established by the legislation in force. The main missions executed in this context are search and rescue, the saved persons air, land, maritime and river transportation, the provision of the necessary infrastructure to use the search and rescue means belonging to other institutions, the conduct of air-medical, forest fire fighting missions, the participation in interventions in the event of emergency situations as well as in joint

[30] Marian Zulean, *Diferențe culturale dintre armată și societatea românească*, Editura Universității Naționale de Apărare, București, 2005, p. 62.

[31] *Ibidem*, p. 19.

[32] *Law on National Defence no. 45/1994*, subsequently amended, *Government Emergency Ordinance no. 21/2004 on the National System of Emergency Situations Management*, approved with amendments and completions by *Law no. 15/2005*, with subsequent amendments, *Government Decision no. 94/2014 on the Organisation, Functioning and Componence of the National Committee for Special Emergency Situations*, with subsequent amendments, *Government Decision no. 2.288/2004, Government Decision no. 1/2014*, related to emergency situations management, *Government Emergency Ordinance no. 21/2004 on the National Emergency Situations Management System*, approved by *Law no. 104/2014*, with subsequent amendments.

ROMANIAN MILITARY THINKING

exercises. The support provided for the central or local administration can be also materialised in aid or services involving military personnel and assets. Through this type of military actions temporary support is provided for civilian authorities, when unpredicted situations occur, which exceed the reaction and response capacity of the entities designated to intervene and solve the type of specific situation.

A concrete example is the support provided for the Ministry of Transportation so that the railway and air transportation could be properly conducted in the situation in which the civilian specialised personnel were on strike, resulting in the normal transportation activity diminishing by more than 2/3.

The restoration of public order, constitutional order and the respect of the law represent other examples of military actions meant for supporting the Ministry of Internal Affairs, the authority empowered by law to manage such situations, under the conditions in which the latter would be overwhelmed by the situation.

The restoration of public order, constitutional order and the respect of the law represent other examples of military actions meant for supporting the Ministry of Internal Affairs, the authority empowered by law to manage such situations, under the conditions in which the latter would be overwhelmed by the situation.

The third type of actions in which the armed forces are employed is represented by ensuring the protection of citizens lives as well as of the public and private property, simultaneously with eliminating the consequences of natural disasters or accidental catastrophes caused by human activity.

Concretely, to provide public services, in compliance with the Constitution, the Ministry of National Defence cooperates with the Ministry of Internal Affairs to:

- provide the public service of ensuring the fluent and secure transportation on public roads;
- hand in the mobilisation orders or clarify the military situation of reservists, in cooperation with zonal military centres;
- save and evacuate the persons and goods damaged by fire, explosion, malfunction, accidents, epidemics, natural disasters and catastrophes;
- limit and remove the consequences of such events[33].

The Ministry of National Defence ensures, in compliance with national legislation:

- the public emergency medical assistance service and qualified first aid, medical and veterinary assistance – referring here to providing public emergency medical care in the pre-hospitalized phase through own ambulance services and to providing public emergency medical care in the hospitalized phase through hospitals in own healthcare network;
- the enhancement of the military and civilian personnel quality of life;
- the provision of religious assistance and of social assistance;
- the public services in the field of military, defence, public order and national security education at high-school, pre-university and university level.

Mention should be made that the military support for civilian authorities is provided exclusively on the national territory, under the authority of the National Military Command Centre[34].

Mention should be made that the military support for civilian authorities is provided exclusively on the national territory, under the authority of the National Military Command Centre.

As for the use of military forces to provide support for other authorities, it is possible only in certain situations, according to the mandate issued by the prosecutor, in compliance with the legal framework[35].

As for the use of military forces to provide support for other authorities, it is possible only in certain situations, according to the mandate issued by the prosecutor, in compliance with the legal framework.

With regard to the military support provided for civilian authorities, there are numerous examples more or less known to the public. Thus, in the event of the catastrophic floods in our country in 1970, 1975, 1999, as well as more recently, the armed forces have intervened using the assets in the inventory (different types of boats, amphibians, vans and helicopters) to save the affected citizens in areas where their lives were endangered. Moreover, the armed forces transported and delivered food, clothes, tents, medicines, potable water for the population, built and managed temporary camps for the population without houses, the troops participated in protecting artworks (bridges, viaducts, portions of roads and railways, tunnels etc.) in the way of the floods, by building or consolidating dams, and they also took part effectively in restoring the communications affected by floods.

In the event of massive snowfall, the armed forces participated in unlocking the communication routes covered by snow and in supplying basic food for the population.

[33] Art. 26, Para. (25), (26) in *Law no. 218/2002 on the Organisation and Functioning of the Romanian Police Forces*, with subsequent amendments and completions.

[34] See http://www.defense.ro/comandamente/cnmc, retrieved on 12 June 2019.

[35] *Government Emergency Ordinance no. 1/1999 on the State of Siege and the State of Emergency*, Romanian Government, *Official Gazette of Romania*, no. 22, on 21.01.1999.

ROMANIAN MILITARY THINKING

Moreover, in the event of earthquakes, such as the one in 1977, the armed forces intervened to save the lives of the citizens caught under the rubble as well as the goods in the damaged or destroyed buildings. The armed forces also provided protection for such goods and other damaged objectives, to prevent the theft of public and private assets[36].

Humanitarian missions using the aircraft belonging to the Romanian Air Force are no longer a novelty. Case by case, flight and medical assistance crews do their best to rapidly and safely transport critically ill patients to the hospitals where their lives can be saved. The missions are executed at the request of the Emergency Situations Department within the Ministry of Internal Affairs[37].

An eloquent example in the practice of other armed forces can be the nuclear disaster produced in 1986, following the explosion occurred in one of the reactors at the nuclear power plant in Chernobyl, Ukraine. Initially, only military troops intervened to evacuate the personnel and the population in a 30-km area around the nuclear plant. Subsequently, the concrete sarcophagus under which the reactor was buried was built by the military personnel too, aspect that unfortunately resulted in casualties among the troops participating in the mission[38].

According to the plans for the joint intervention of the units belonging to the Ministry of National Defence and to the Ministry of Internal Affairs to limit and eliminate the effects of disasters on the national territory, in the 2017-2018 period, they conducted 160 training activities in 30 counties and in Bucharest, in which were involved about 6,000 troops and more than 7,000 technical assets.

Military Support for Civilian Authorities – Case Studies

The actions jointly conducted with the structures belonging to the Ministry of Internal Affairs consist of alert exercises and actions with forces and assets on the ground.

According to the plans for the joint intervention of the units belonging to the Ministry of National Defence and to the Ministry of Internal Affairs to limit and eliminate the effects of disasters on the national territory[39], in the 2017-2018 period, they conducted 160 training activities in 30 counties and in Bucharest, in which were involved about 6,000 troops and more than 7,000 technical assets.

[36] Teodor Frunzeti, *Acțiunile militare altele decât războiul*, Editura Academiei Forțelor Terestre, Sibiu, 2000, pp. 91-95.

[37] Air Force Journal – *Cer Senin*, published by the Air Force Staff, Bucureşti, no. 2/2019, p. 17.

[38] Teodor Frunzeti, *op. cit.*, p. 93.

[39] In compliance with the Supreme Council of National Defence Decision no. S/128/2005, the units belonging to the Ministry of National Defence and the Ministry of Internal Affairs develop the *Joint Intervention Plan* and, based on it, semester information related to the activities conducted in the field of emergency situations.

romania2019.eu

The mentioned actions were aimed at enhancing the common interventional picture, testing the information-decision flow, and assessing the intervention capabilities pre-established through the action plans according to the types of risks/cooperation for the limitation and elimination of disaster effects.

The actions were conducted in various environments that ensured the conditions for the assessment to meet the objectives established in the planning documents, and they were aimed at:

- consolidating the relations with the specialised bodies in the central and local public administration, and with nongovernmental organisations;
- participating with forces and logistic support in eliminating the effects of natural disasters or technological accidents;
- conducting actions for the benefit of the population (transportation, accommodation, food, medical assistance, access to isolated areas, humanitarian aid);
- - protecting cultural objectives and civil population, at the request of responsible public authorities;
- providing support for ensuring the continuity of vital communication capabilities and protecting critical infrastructure elements as well as economic objectives running highly potential biological, chemical, radiological or nuclear risks;
- participating in the actions meant for localising, isolating and extinguishing fire, in support of specialised forces belonging to other institutions.

In the analysed period (2017-2018), there were jointly executed intervention missions to reduce the consequences of extreme meteorological phenomena, in which about 1,600 troops and more than 180 specific technical assets participated.

Moreover, in the analysed period (2017-2018), there were jointly executed intervention missions to reduce the consequences of extreme meteorological phenomena, in which about 1,600 troops and more than 180 specific technical assets participated[40].

Another concrete example in terms of the support provided for civilian authorities is the mission in 2011 to evacuate the Romanian and other nationalities citizens from the Libyan Arab Jamahiriya, following the crisis there. At that moment, based on a government decision, it was established a crisis cell at the level of the Ministry

40 In compliance with the information provided by the Ministry of National Defence and the Ministry of Internal Affairs during the 2017-2018 period.

of National Defence, intended to identify the solutions so that the Romanian Armed Forces could participate in the mission in cooperation with the Ministry of Foreign Affairs. Two aircraft belonging to the Romanian Air Force were made available to create a true air bridge between Bucharest and Tripoli, in the period 24 February – 1 March 2011. A complete military, diplomatic and consular mechanism was employed to ensure the success of the first air mission to evacuate some Romanian citizens in danger in a foreign country after the Second World War. The two C-130 Hercules and C-27J Spartan military aircraft executed, in total, seven missions on the Bucharest – Tripoli route as well as a series of evacuation operations between Tripoli and La Valletta. Thus 230 persons were evacuated. Among them, 175 were Romanian citizens, the rest having other nationalities. In turn, other countries assisted the Romania citizens, based on the activation of the Monitoring and Information Centre within the European Union Civil Protection Mechanism[41].

Conclusions

Following the presented analysis, it can be stated that, from the current doctrinal perspective and through the prism of the conducted activities, the armed forces meet the characteristics of public services, be they either *"old"* or *"social".*

Moreover, if we take into account the legislative framework, the armed forces represent a system that, in terms of its nature, can be categorised as an administrative public service, and, in terms of its destination, can be considered one of the public services for the benefit of the community in its aggregate.

In terms of the possibility of delegation, the armed forces are considered a service that cannot be delegated. In terms of its social importance, the service is among vital public services, and, in terms of its scope, it meets the necessary conditions to be considered a public service of national importance.

It is also noted the evolution of the concept of civil-military relation, from the purely realistic vision of Plato, who imagines the military in the strict role of *"guardian of the City"*, to the professional military in democratic societies, the liberal model, standing out for expertise, responsibility and corporatism, playing a much more complex role in the society to which he/she belongs. Freed from the doctrinal limitation specific to mass armed forces, built based on the communist model, the Romanian Armed Forces have transformed and adapted to the rigours of modern, professional, armed forces, becoming a fundamental institution of the rule of law.

On the other hand, the public service, as an activity, is indissolubly linked to the idea of general interest and the will of the public authorities that decide when and how the interest can be met.

Considering all the presented aspects, we conclude, without fear of being wrong, that the Romanian Armed Forces have all the characteristics of a public service, being the guarantor of national sovereignty and independence, of territorial unity and integrity, significantly contributing to regional and global stability and security.

The Romanian Armed Forces have all the characteristics of a public service, being the guarantor of national sovereignty and independence, of territorial unity and integrity, significantly contributing to regional and global stability and security.

BIBLIOGRAPHY

1. ***, *Constitution of Romania*, Chapter V, Section 1, Article 118 – Armed Forces, https://www.constitutia.ro/art-118-fortele-armate.htm.
2. ***, *Budapest Summit Declaration*, CSCE, *Budapest Document 1994, Towards a Genuine Partnership in a New Era*, www.osce.org/mc/39554?download=true.
3. ***, *Government Decision no. 94/2014 on the Organisation, Functioning and Componence of the National Committee for Special Emergency Situations*, with subsequent amendments.
4. ***, *Government Decision no. 2.288/2004 on the Approval of the Main Support Functions Ensured by Ministries, Other Central Bodies, and Non-Governmental Organisations to Prevent and Manage Emergency Situations.*
5. ***, *Law on National Defence no. 45/1994*, with subsequent amendments.
6. ***, *Law no. 15/2005*, with subsequent amendments.
7. ***, *Operational Law Handbook*, The Judge Advocate General's Schools Charlottesville, Virginia, 2010.
8. ***, *Government Emergency Ordinance no.1/2014 on Some Measures in the Field of Emergency Situations Management*.
9. ***, *Government Emergency Ordinance no. 21/2004 on the National System of Emergency Situations Management*, approved with amendments and completions.

41 Air Force Journal – *Cer Senin*, published by the Air Force Staff, Bucureşti, no. 1/2011, pp. 6-7.

10. ***, *Government Emergency Ordinance no. 1/1999 on the State of Siege Regime and the State of Emergency Regime*, the Government of Romania, published in the *Official Gazette of Romania*, no. 22, on 21.01.1999.
11. ***, *Regulations on the Chamber of Deputies*, approved through the Chamber of Deputies Decision, no. 8/1994, synthesis – 10 June 2019, Chapter IV, p. 28, see http://www.cdep.ro/pdfs/tab_acte/Regulament-din-1994-forma-sintetica-pentru-data-2019-06-10.pdf.
12. ***, Air Force Journal – *Cer Senin*, published by the Air Force Staff, Bucureşti, no. 2/2019, no. 1/2011.
13. Barbu Brezianu, *Gruparea Arta Română*, in *Studii de istoria artei*, Plastic Arts Series, Volume 11, no. 1, 1964.
14. J. Chevallier, *Le Service Public*, Presses Universitaires de France, Paris, 1994.
15. George-Dorinel Dumitru, Dragoş-Adrian Bantaş, *Controlul democratic asupra sectorului de securitate – privire comparativă asupra modelului european şi aplicării acestuia în România*, in *Gândirea Militară Românească* Journal, Edition 1-2/2018, published by the Defence Staff, Bucureşti.
16. Petre Duțu, *Armata şi societatea în tranziție*, Editura Academiei de Înalte Studii Militare, Bucureşti, 2002.
17. Teodor Frunzeti, *Acțiunile militare altele decât războiul*, Editura Academiei Forțelor Terestre, Sibiu, 2000.
18. Samuel P. Huntington, *The Soldier and the State. The Theory and Politics of Civil-Military Relations*, The Belknap Press of Harvard University Press Cambridge, Massachusetts, London, 1957.
19. Antonie Iorgovan, *Tratat de drept administrativ*, vol. I, Editura Nemira, 1996.
20. Jacqueline Morand-Deviller, *Cours de Droit administratif. Thèmes de réflexion. Commentaires d'arrêts avec corrigés*, VII-ème édition, Paris I, Sorbonne.
21. Paul Negulescu, *Tratat de drept administrativ*, Tipografiile Române Unite, București, 1925.
22. Daniel N. Nelson, *Definition, Diagnosis, Therapy – A Civil-Military Critique*, Defense&Security Analysis, vol. 18, 2002, no. 2.
23. Doina Talaşman, *Considerații privind raporturile dintre istorie şi sociologie, respectiv armată şi societate*, in *Armata română şi societatea civilă*, studies presented at the Scientific Papers Session dedicated to the Military Archives Day, on the anniversary of 92 years since the establishment of the Centre for the Study and Preservation of Historical Military Archives and 145 since the establishment of the Armed Forces Historical Service, coordinators: Colonel Marian Moşneagu, PhD, Colonel Petrişor Florea, PhD, Cornel Țucă, PhD Editura Istros, Piteşti, 2012.

24. Major (mil. just) Cristina Ştefan Nicolaie, *Dreptul afacerilor civile în operații militare* (rezumat), Bucureşti, 2015.
25. Marybeth Peterson Ulrich, *Democratizing Communist Militaries: The Cases of the Czech and Russian Armed Forces*, Michigan, University of Michigan Press, 1999.
26. Marin Văraru, *Tratat de drept administrativ român*, Editura Librăriei Socec & Co., Bucureşti, 1928.
27. Andrei Vocilă, *Dinamica fenomenului militar românesc după 1990 în relație cu factorul politic şi social*, see https://andreivocila.wordpress.com/2010/11/08/dinamica-fenomenului-militar-romanesc-militar-romanesc-dupa-1990-in-relatie-cu-factorul-politic-si-social/
28. Marian Zulean, *Armata şi societatea în tranziție*, Editura Tritonic, Bucureşti, 2003.
29. Marian Zulean, *Diferențe culturale dintre armată şi societatea românească*, Editura Universității Naționale de Apărare, Bucureşti, 2005.
30. Marian Zulean, *Militarul şi societatea. Relațiile civil-militare la începutul mileniului al III-lea*, Editura Militară, Bucureşti, 2008.

WEBOGRAPHY

1. https://armed.mapn.ro/nicolae-grigorescu-pictor-de-razboi-2326-23.
2. http://www.defense.ro/comandamente/cnmc
3. http://enciclopediaromaniei.ro/wiki/Mihail_Sadoveanu.
4. https://www.viata-libera.ro/prima-pagina/118267-centenarul-marii-uniri-pictori-si-sculptori-in-primul-razboi-mondial.

LEADERS EDUCATION – DECISIVE FACTOR IN EFFECTIVE ORGANISATIONAL LEADERSHIP –

Cosmin BUȚA
Master's student, "Carol I" National Defence University

A complex phenomenon, part of organisational management, leadership is both art and science. There are many definitions of the term mentioned by the author in the present paper, pertinent and probative examples being provided. Leadership is present in any structure, and especially in the military one, considering that the existing relations between commanders and subordinates are established by military regulations. In this context, the article emphasises a series of characteristics of the system of connections in a military organisation, all of them based on discipline, respect, responsibility, trust and loyalty.

Moreover, the author stresses the importance of leaders education for their life-long learning. Thus, a leader will be effective and adapted to any change in the organisation. Last but not least, an educated leader will motivate the subordinates in their actions, be they related to conception, training or combat.

Keywords: leadership, responsibility, subordinate motivation, theatre of operations, education.

English version by **Diana Cristiana LUPU**.

Motto:

"Army leaders in this century need to be Pentathletes, multi-skilled leaders who can thrive in uncertain and complex operating environments …, innovative and adaptive leaders who are expert in the art and science of the profession of arms. The Army needs leaders who are decisive, innovative, adaptive, culturally astute, effective communicators, and dedicated to life-long learning"[1].

Introduction

Current society undergoes a continuous development process, and the military factor cannot be an exception from the mentioned desideratum. The realities in the confrontation areas have proved that success has been determined by at least two variables: time and space. Based on this premise, actions happen at a rate that, unfortunately, very often, exceeds the commanders capacity to react in due time so that the troops action can be efficient and generate effects on the enemy or counter its actions. In this regard, the education of the human resource having responsibilities in the field of *leadership*, on the one hand, and the education of the subordinates in the field of *followership*, on the other hand, have become necessary.

The concept of leadership has acquired, throughout time, different valences, being studied by researchers, businessmen, sports teams as well as by the military personnel.

The concept of *leadership* has acquired, throughout time, different valences, being studied by researchers, businessmen, sports teams as well as by the military personnel. Although, practically, it is available to all of us, in each and every habitual action, and *"certainly, it can be recognised when noticed"*[2], *leadership* seems difficult to define. Thus, there are experts stating that *leadership* represents *"one of the most studied and least understood phenomena on earth"*[3].

[1] Francis J. Harvey, Secretary of the Army, speech for US Army Command and General Staff College graduation, in Langston J. Turner, *Developing Army Leaders through Increased Rigor in Professional Military Training and Education*, Fort Leavenworth, Kansas, 2017.

[2] Colonel Bernd Horn, Robert W. Walker, PhD *The Military Leadership Handbook*, Dundurn Press, Kindle Edition, 2008, p. 5.

[3] James McGregor Burns, *Leadership, Harper&Row*, New York, 1978, *apud* Mielu Zlate, *Leadership și management*, Editura Polirom, 2004, p. 13.

ROMANIAN MILITARY THINKING

Military *leadership*, although it is rigorously established and organised through the existing relations within a military structure, cannot be an exception from what has been previously mentioned. This idea is firstly generated by the absence, in the Romanian Armed Forces doctrinal regulations, of an explicit definition for what other modern armed forces call *effective military leadership*, *"motivating and empowering subordinates to professionally and ethically fulfil their mission while developing and improving the capabilities that contribute to its success"*[4].

The experience acquired in the theatre of operations and in the multinational exercises conducted with partners in the North Atlantic Treaty Organisation has shown that modern military leaders command forces using a series of concepts on maps. Moreover, it has been noted that there are military leaders that create instruments to support decision during the planning process.

The experience acquired in the theatre of operations and in the multinational exercises conducted with partners in the North Atlantic Treaty Organisation has shown that modern military leaders command forces using a series of concepts on maps. Moreover, it has been noted that there are military leaders that create instruments to support decision during the planning process. They early transform the information received in *OPORD (Operations Order*) from the superior echelon into means to support the military command structure and decisively influence the action by reducing the command reaction time, the personnel training long before the event as such, and the forces organised action. The estimation of the decision points even since the planning period helps both the commander and the staff. Thus, we can speak of an organised and scientifically documented reaction, which is the military leader attribute.

The Multidisciplinary Character of the Leadership Concept

The first studies in modern *leadership* were focused on leaders analysis[5] and were conducted at the beginning of the 20th century by American psychologist Lewis Madison Terman. From that moment on, there have been published many analyses, studies and articles, successively explaining leaders personal characteristics, analysing *leadership* in terms of specific actions and functions, and researching *leadership* from the standpoint of organisations dynamics and social influence.

Thus, in 1960, Professor Bernard Morris Bass developed a theory according to which it is not enough for a leader to exercise the act of command. Moreover, he/she should also be positive and efficient: *"When the purpose of member A is to change B (within a group), the efforts made by A mean an attempt to exert leadership; B can indeed change behaviour as a result of A's attempts, this will be the positive leadership function. B's change can bring A's satisfaction..., this will be the effective leadership function"*[6].

romania2019.eu

In 1960, Professor Bernard Morris Bass developed a theory according to which it is not enough for a leader to exercise the act of command. Moreover, he/she should also be positive and efficient: "When the purpose of member A is to change B (within a group), the efforts made by A mean an attempt to exert leadership; B can indeed change behaviour as a result of A's attempts, this will be the positive leadership function. B's change can bring A's satisfaction..., this will be the effective leadership function"

By this example, *leadership* is included among the phenomena having social influence; however, it is assessed as effective only in dependence on the leader's satisfaction. Subsequently, in 1961, it was defined, for the first time, the instrument through which social influence is exercised, namely *communication*: *"Leadership is the interpersonal influence exercised in a defined and guided situation, due to the communication processes, to meet a determined goal or goals"*[7]. Further on, it was debated the idea according to which the influence exercised by the leader to meet a goal could be compliant or not with the organisation goal: *"our definition of leadership is that it appears whenever a person attempts to influence the behaviour of another person or a group, regardless the motive. It can be related to own or other goals, and these goals can be congruent or not with the organisational goals"*[8].

Nowadays, *leadership* is analysed in much more complex terms, considering factors such as: commander's vision, responsibility, influence, priorities, ability to contribute to subordinates development and to enhance their self-confidence etc. Thus, current theories emphasise that the first and foremost responsibility of a leader is to define the reality in which he/she conducts the activity and to understand it. The last responsibility is to thank the subordinates. Between the two responsibilities, the leader should exercise, within the structure, all the necessary qualities to meet the group objective, to enhance the quality of the professional act, to maintain a high level of motivation among the subordinates, and to create a positive work environment. Meanwhile, the following questions arise: *Have the members of the group reached their maximum potential?, Can they*

[4] ***, *Doctrine, Leadership in the Canadian Forces: Conceptual Foundations*, Department of National Defence (DND), Kingston, 2005, p. 30.

[5] Lewis Madison Terman, *A Preliminary Study of the Psychology and Pedagogy of Leadership*, in *Journal of Genetic Psychology*, Penguin Books, London, 1969, p. 34.

[6] Bernard Morris Bass, *Leadership, Psychology and Organizational Behavior*, Harper, New York, apud Mielu Zlate, *op. cit*., p. 23.

[7] R. Tannenbaum, I.R. Weschler, F. Massarik, *Leadership and Organization*, McGraw-Hill, New York, p. 24, apud Mielu Zlate, *op. cit.*, p. 23.

[8] P. Hersey, K.H. Blanchard, D.E. Johnson, *Management of Organizational Behavior. Leading Human Resources*, VIIth ed., Prentice Hall, New Jersey, p. 9, apud Mielu Zlate, *op. cit.*, p. 25.

have the required results?, Are they enough motivated so that the group can meet the objectives?, Are they contented? Such questions represent the first signs that the exercised *leadership* is constructive, a premise for obtaining remarkable results.

On the other hand, the relation between the leader and the changes that occur in the structure can also result in progress or regress. The difference between the two types of results is made by the way in which the leader understands the situation, approaches change, and decides to act to implement his/her plan. However, all the mentioned aspects require the leader's involvement in accepting the new situation, although sometimes it creates discomfort. In this regard, Dan Sweeney, an IBM adviser and employee, states that *"Changes entail reconsidering priorities and hard work..., invalidate previous decisions and force us to make more appropriate ones. They discredit previous objectives and aspirations and force us to target new ones. Change makes us reprioritise..."*[9]. In this context, I consider that a leader that trusts his/her people and decides to approach change together with them will be much more successful than one that tries to avoid the problem, hoping that it will pass. In such situations, the leader should have a plan, a strategy for change. Otherwise, it is possible that change can generate a series of difficulties in the act of management.

The relation between the leader and the changes that occur in the structure can also result in progress or regress. The difference between the two types of results is made by the way in which the leader understands the situation, approaches change, and decides to act to implement his/her plan. However, all the mentioned aspects require the leader's involvement in accepting the new situation, although sometimes it creates discomfort.

Other authors have analysed the results obtained by leaders starting from the connection between them and their subordinates, on the one hand, and between them and those with whom they cooperate, on the other hand. Thus, John C. Maxwell, one of the most famous modern authors in the field of *leadership*, considers that no leader is able to succeed alone. His/her success depends, to a large extent, on the quality of the people around him/her[10]. Most leaders naturally create a network formed by people they like or make them feel comfortable. Other leaders consider the way in which those near them effectively contribute to the development of their leadership potential or to the importance of exercising their influence on the people who can, in turn, influence others, thus multiplying the effects of *leadership*. The same John C. Maxwell considers that the *leaders that prefer having around people who permanently agree with their decisions or who excessively feed their ego cannot be successful in the*

[9] Oren Harari, *Secretele lui Colin Powell*, Editura Tritonic, București, 2006, p. 81.

[10] John C. Maxwell, *The 21 Irrefutable Laws of Leadership*, 10th Anniversary Edition, Nashville, Tennessee, Thomas Nelson, 2007, pp. 127-141.

long run as the leader's potential is determined by the quality of the people around. In this respect, *leadership* expert Warren Bennis states that the *"leader finds his/her greatness in the group and helps each member to find it in himself/herself"*[11].

The diversity of the *leadership* concept definitions often denotes a reflection on the differences between the environments in which it is present. In this regard, it is very clear the fact that the concept is defined in one way in the military environment and in another way in the economic, sports or political environment. To different degrees, the definitions of the *leadership* concept tend to be limited from the functional and cultural perspective. Therefore, some definitions are restricted to qualifying the importance of the leader's formal authority, while others intercondition the success achievement and the subordinates contribution, or emphasise the importance of a common or group objective. However, in the doctrine of the Canadian Armed Forces, for example, it is analysed as follows: *"leadership can be generally defined as a process to directly or indirectly influence the others by the exercise of the official authority/attribute of a person and by the creation of motivation to act ethically and in compliance with the group common intention or goal"*[12].

Leadership has been debated and understood in different modes, depending on the way of thinking of those analysing the concept and the related system of values. The main difference in terms of the way of interpreting and analysing leadership, in general, and military leadership, in particular, is that the latter has been debated by experienced military practitioners in relation to what can be called leadership applied in military conflicts.

Particularities of Military Leadership and the Necessity of Education

Leadership has been debated and understood in different modes, depending on the way of thinking of those analysing the concept and the related system of values. The main difference in terms of the way of interpreting and analysing *leadership*, in general, and military *leadership*, in particular, is that the latter has been debated by experienced military practitioners in relation to what can be called *leadership* applied in military conflicts. Thus, if Marshal Montgomery emphasises the ability and will to put people together for a common goal[13], General George S. Patton considers that the most important

[11] Warren Bennis, *Organizing Genius: The Secrets of Creative Collaboration*, Perseus Books, New York, 1998, apud Mielu Zlate, *op. cit.*, p. 13.

[12] ***, *Conceptual Foundation, Leadership in the Canadian Forces: Conceptual Foundations*, DND, *op. cit.*, p. 8.

[13] *"Leadership: The Capacity and Will to Rally People to a Common Purpose Together with the Character that Inspires Confidence and Trust"*, Field Marshal Montgomery, see www.ctm.uca.edu.au/living-leadership/leadership-is/leadership/leadership-is/, retrieved on 01.02.2019.

quality of a leader is the ability to make decisions[14]. General Dwight D. Eisenhower, in turn, considers fostering the subordinates motivation to meet the shared objectives[15] is the most important quality of a leader. We therefore note that three great leaders that commanded the allied forces in Europe simultaneously, being on the same side of the barricade, provided different definitions for the *leadership* concept. Subsequently, as the military science and art developed, new theories emerged, such as the one of General Norman Schwarzkopf, emphasising character and the ethical component of decisions[16].

Jim Collins, expert in the field of business and company management, has studied, for approximately two decades, the way in which certain institutions succeed in obtaining superior results. He states that the leaders "who have understood the transformation from good to great have not firstly established the route of the bus and then the appropriate people to get on it. No, they firstly found the appropriate people".

Following a simple analysis of these conceptual delineations, we can conclude that the interpretations of the term *leadership* are complementary, and accepting one definition does not exclude the other ones. I consider that the significance of this concept resides in the leader's art to combine the mentioned variables to successfully fulfil the mission.

Jim Collins, expert in the field of business and company management, has studied, for approximately two decades, the way in which certain institutions succeed in obtaining superior results. He states that the leaders *"who have understood the transformation from good to great have not firstly established the route of the bus and then the appropriate people to get on it. No, they firstly found the appropriate people"*[17]. In other words, the *team is key and, before developing objectives, missions and plans, an organisation should find the people that fit the projects it intends to develop*, as a person who does not fit the team can counter a very well developed plan.

The current military doctrines related to *leadership* focus on the theory of leadership by example. For a long period of time, it has been considered that personal example is the best argument to determine subordinates to execute orders in an effective manner. It is a necessary but not sufficient condition for the motivation of

[14] *"Be willing to make decisions. That's the most important quality in a good leader"*, General George S. Patton.

[15] *"Leadership: the Art of Getting Someone Else to Do Something You Want Done because He Wants to Do It"*, Dwight D. Eisenhower, US President (1890-1969), see www.ctm.uca.edu.au/living-leadership/leadership-is/leadership/leadership-is/, retrieved on 01.02.2019.

[16] *"Leadership is a combination of strategy and character. If you must be without one, be without the strategy"*, General H. Norman Schwarzkopf, see www.ctm.uca.edu.au/living-leadership/leadership-is/, retrieved on 01.02.2019.

[17] J. Collins, *Good to Great*, New York, NY: Harper Collins Publishers, 2001, p. 39, apud Dwayne G. Hodges, *An Executive Position on Military Leadership*, Wilmington University, August 2012, p. 32.

subordinate personnel to execute a combat mission. *Modern military leader develops mutually loyal relations with subordinates and treats them with respect and appreciation*[18]. The military experience in the past years have demonstrated the fact that there is a cause-effect relationship between the leader's attitude towards subordinates and their determination to obey the orders. Thus, John Maxwell considers that *one of the factors subordinates relate to when they interact with the command personnel does not have anything in common with what the leader thinks about them or with the leader's capacity to command. Each and every subordinate wonders if the leader cares for him/her or not*[19]. According to this theory, the moment the leader proves, through his/her actions, that subordinates are very important both for him/her and for the group they belong to we can speak about the emergence of the first conditions for the development of performant *leadership*.

Current military leader often acts in a multinational and joint environment, and it is the main reason why his/her education in terms of speaking foreign languages is related to the organisational culture of those with whom he/she interacts. Moreover, the ability to negotiate is also important. All the mentioned aspects represent qualities that can be developed through education.

Other analysts such as Montor, McNicholas, Ciotti, Hutchinson and Wehmueller[20] consider that *a decisive factor for a good leader is his/her education.* This requirement refers to the leader's ability to identify the existing problems, to analyse them, and to express clearly and concisely. Current military leader often acts in a multinational and joint environment, and it is the main reason why his/her education in terms of speaking foreign languages is related to the organisational culture of those with whom he/she interacts. Moreover, the ability to negotiate is also important. All the mentioned aspects represent qualities that can be developed through education.

Considering education, some questions arise as follows: *Why are some leaders performant and others are not?, How could, in the first part of the Second World War, commanders such as Marshal Erich von Manstein, Heinz Guderian or Erwin Rommel win decisive victories when confronted with pretty well prepared armed forces?*, It is well known that, besides the technological factor, the tactical doctrine or the available resources, one of the most important factors that influenced the course of the Second World War was the *leadership*

[18] F.R. Kirkland, *Leadership Doctrine: 1778 to 1995*, in *Military Review*, 78(1), 1998, pp. 30-40, apud James P. Butler, *Positive Leadership in the Military: an Exploratory Study*, Capella University, September 2011, p. 40.

[19] www.johnmaxwellteam.com/2019-care/?c=jmax-wp-bo&jmtc=mwm-word&jmta=mwm-word-care/, retrieved on 08.02.2019.

[20] K. Montor, T.M. McNicholas, A.J. Ciotti, T.H. Hutchinson, J.E. Wehmueller, *Naval Leadership: Voices of Experience*, Annapolis, MD: Naval Institute Press, 1987, apud James P. Butler, *op. cit.*, p. 43.

practised by the German forces. Through that form of *leadership*, authority was delegated up to the bottom levels of decision, so that the decision made by a platoon or company commander in order to fulfil the mission din not have to be agreed to as far as it was compliant with the hierarchical commander intention and it was within the limits imposed by him. Starting with the second part of the Second World War, the Allies noted the German superiority at doctrinal level and the fact that they were able to make decisions and act more rapidly than the British or French forces could do. The Germans were able to develop, up to the bottom level, what their adversaries called *Führen mit Auftrag/mission-oriented leadership* or *Auftragstaktik/command through missions.*

For a long period of time, it has been considered that the military leader, through his/her innate qualities, has had available enough instruments to successfully command forces. However, it has been noted that on-the-spot decisions are less effective than those adopted following a decision-making process. In other words, the unilateral decision, made by a single commander, is, more often than not, doomed to failure, compared to a decision made by a leader that accepts expert advice.

For a long period of time, it has been considered that the military leader, through his/her innate qualities, has had available enough instruments to successfully command forces. However, it has been noted that on-the-spot decisions are less effective than those adopted following a decision-making process. In other words, the unilateral decision, made by a single commander, is, more often than not, doomed to failure, compared to a decision made by a leader that accepts expert advice. In this regard, Harold D. Koontz, one of the promoters of organisation theory, states that *if a leader is passive towards this rapidly developed science, he/she can be almost certain that, in time, he/she can be at the disposal of another leader who learns it*[21].

In modern armed forces the leaders education process is based on educational doctrines and strategies dedicated to *leadership*. In this regard, to perform and to adapt to the ever-changing situations, nowadays, military leaders should develop both critical and creative thinking abilities, in order to note the change, to interpret it, and to intervene together with the subordinate staff. This concept will be better understood and adopted by a commander if he/she accepts that it is much more effective to lead with the help of his/her staff and the subordinate leaders, delegating authority and by substantiating his/her decisions following the advice provided by his/her experts, and by creating those instruments that help in exercising the act of command.

[21] Harold Koontz, *Conducerea activității economice în accepțiunea modernă*, in H.B. Maynard, *Conducerea activității economice*, Editura Tehnică, București, 1972, p. 43, translated by Eng. Silvia Zamfirescu.

Conclusions

Promoting performant *leadership* does not limit to the act of command as such or to the innate qualities of a leader. To meet performance in an environment characterised by change, volatility and ambiguity, leaders should have access to education. This way, they can develop an effective work environment, based on promoting the subordinates self-confidence, assuming responsibilities by all members of the organisation, and sharing risks in an equitable manner. Meeting this desideratum positively influences the winner spirit of the people and their will to seek success. In this regard, Oren Harari, in *"The Leadership Secrets of Colin Powell"*, states one of the principles of the US Secretary of State: *"If you believe that your people are professionals and transmit it, they really become performant!"*[22].

To meet performance in an environment characterised by change, volatility and ambiguity, leaders should have access to education. This way, they can develop an effective work environment, based on promoting the subordinates self-confidence, assuming responsibilities by all members of the organisation, and sharing risks in an equitable manner.

BIBLIOGRAPHY

1. James P. Butler, *Positive Leadership in the Military: an Exploratory Study*, Capella University, September 2011.
2. Oren Harari, *Secretele lui Colin Powell*, Editura Tritonic, București, 2006.
3. Colonel Bernd Horn, Dr Robert W. Walker, *The Military Leadership Handbook*, Dundurn Press, Kindle Edition, 2008.
4. Dwayne G. Hodges, *An Executive Position on Military Leadership*, Wilmington University, August 2012.
5. H. Koontz, *Conducerea activității economice în accepțiunea modernă*, in H.B. Maynard, *Conducerea activității economice*, Editura Tehnică, București, 1972.
6. John C. Maxwell, *The 21 Irrefutable Laws of Leadership*, 10th Anniversary Edition, Nashville, Tennessee, Thomas Nelson, 2007.
7. Lewis Madison Terman, *A Preliminary Study of the Psychology and Pedagogy of Leadership*, in *Journal of Genetic Psychology*, Penguin Books, London, 1969.
8. Langston J. Turner, *Developing Army Leaders through Increased Rigor in Professional Military Training and Education*, Fort Leavenworth, Kansas, 2017.
9. Mielu Zlate, *Leadership şi management*, Editura Polirom, 2004.
10. ***, *Conceptual Foundation, Leadership in the Canadian Forces: Conceptual Foundations*, DND, Kingston, 2005.
11. ***, *Doctrine, Leadership in the Canadian Forces: Conceptual Foundations*, DND, Kingston, 2005.
12. ***, www.ctm.uca.edu.au, retrieved on 01.02.2019.
13. ***, www.johnmaxwellteam.com, retrieved on 08.02.2019.

[22] Oren Harari, *op. cit.*, p. 119.

NATO – INTERNATIONAL HUB FOR PROMOTING GENDER PERSPECTIVE WITHIN THE ARMED FORCES

Silvia STANCIU

PhD Student, "Carol I" National Defence University

The reality of contemporary conflicts justifies and implies, within the current military operations, the exploitation of a large array of resources and qualifications that are necessary during the process of assuring international peace and security on the long term. Even since 1961, NATO has become aware of the fact that gender perspective integration at the level of security providers represented a guarantee for the organisational resilience facing numerous international security challenges, as well as a measure of performance within the political and military domain by fully using the human resource. Once with the UNSCR 1325 "Women, Peace and Security" endorsement, in 2000, NATO successively adopted policies, strategies, and action plans designed to promote and implement gender equality within the Alliance structures and also at the level of the member or partner states Armed Forces. In addition, together with its strategic partners, NATO has developed mechanisms meant to apply gender diversity in a comprehensive manner, all with the purpose of raising operational efficiency and enhancing military capabilities. Counting on the importance of collaboration between the evolutions in the weapon industry, military technologies and inclusive capitalisation of the human resource, NATO has succeeded in becoming a modern Alliance, a genuine international hub of gender perspective integration at the level of security and defence.

Keywords: UNSCR 1325, gender integration, international hub, diversity, inclusion.

Introduction

In 1995, UN Secretary General Boutros Boutros-Ghali announced, as a premiere, the fact that the UN was ready to assume its engagement regarding raising the number of women participating in missions under its aegis. Five years later, in October 2000, after several systematic campaigns of the civil society run by the activists for human rights and peace, UN adopted a formalised legal framework of the issue, subsequently submitted as the UN Security Council Resolution 1325 *"Women, Peace and Security".*

At present, together with another seven resolutions adopted across the years (UNSCR 1820 – 2009; UNSCR 1888 – 2009; UNSCR 1889 – 2010; UNSCR 1960 – 2011; UNSCR 2106 – 2013; UNSCR 2122 – 2013; UNSCR 2242 – 2015), the *"Women, Peace and Security"* agenda has become one of the main strengths of NATO, which has chosen to invest a lot of diverse resources in developing this trend considered to be a cardinal aspect for maintaining international peace and security. Contemporary conflicts, generated by hybrid threats, have determined the increase of female influence within the security environment and respectively, the inclusion of gender perspective within peace negotiations, humanitarian actions planning, peacekeeping operations, post-conflict reconstruction and governmental activities. The paradigm shift has induced, as a consequence, a reorganisation of roles, especially within the military domain, which was exclusively open for male expertise only, for a long period of time.

Contemporary conflicts, generated by hybrid threats, have determined the increase of female influence within the security environment and respectively, the inclusion of gender perspective within peace negotiations, humanitarian actions planning, peacekeeping operations, post-conflict reconstruction and governmental activities.

The commitments actively assumed within this direction have transformed NATO in an international hub for gender mainstreaming and also a promoter, through tangible means and with notable results, of the importance related to large-scale capitalisation of gender equality. Being equally a visionary and resilient organisation, with the help of its highly specialised structures, NATO has managed to map the progress registered by the whole Alliance in implementing UNSCR 1325, as well as to set the future trends meant to be

internationally exploited, in order to eliminate discrimination and to diversify the military capabilities involved within missions carried on in complex operational environments.

Legal framework for UNSCR 1325 mainstreaming agenda

The dynamics of international politics has determined a continuous evolution at the NATO level, a fact revealed in concrete terms through the number and depth of the initiatives addressed regarding gender issues. Thereby, in 2007, the North Atlantic Council (NAC), together with Partnership for Peace (PfP) partners, has conceived the first policy of the Alliance, meant to incorporate the will and the efforts of the military authorities in respect to the implementation of UNSCR 1325.

The dynamics of international politics has determined a continuous evolution at the NATO level, a fact revealed in concrete terms through the number and depth of the initiatives addressed regarding gender issues. Thereby, in 2007, the North Atlantic Council (NAC), together with Partnership for Peace (PfP) partners, has conceived the first policy of the Alliance, meant to incorporate the will and the efforts of the military authorities in respect to the implementation of UNSCR 1325.

For the first time, the **NATO/EAPC Policy** recommended the official recognition of the importance given to gender perspective entailment within NATO missions, and tasks member states to develop practical proposals for UNSCR 1325 implementation, concurrently with reporting and following the work undertaken in this field by the United Nations (UN), the European Union (EU) and the Organization for Security and Cooperation in Europe (OSCE). This measure was intended to globally guarantee compatibility of efforts, exchange of experience and development of good practice, all by virtue of ensuring the interoperability between the armed forces of NATO member states.

Additionally, the NATO/EAPC Policy highlighted the major implications deriving from the complexity of the NATO missions and thus required that the incorporation of the gender issue was harmonised with the efforts and contributions of other agencies focused on this field of activity. In 2011, the Policy was revised, gender subject issues being reorganised into four areas of interest, prevention, protection, participation[1] and relief and recovery[2], and on other five key domains highlighted through a Comprehensive Report that was endorsed by member states at the Lisbon Summit[3]. In this new format, the updated policy, along with other reference documents like the Bi-Strategic Directive 40-1 and the NATO/EAPC Action Plan, reiterated the importance of the member states' initiatives, developed within a common legal framework that enabled the further adoption of the national policies and programmes.

Taking into consideration the continuously changing social and political environment, the final policy adopted in 2018 is intended to transpose the global engagements of *"Women, Peace and Security"* within a context adapted to the NATO specific missions and objectives. The accent is thus laid on the principles of integration, inclusiveness and integrity, which correspond to the values that lie at the very core of the Alliance functioning, such as safeguarding individual liberty, defending democracy, respecting human rights and the rule of law. Gender perspective integration, as well as women' inclusion within the whole array of activities attached to the Alliance, represent an essential factor showing the success obtained in the domain of peace conservation in a highly complex security environment. In this regard, the working framework proposed through the new policy is focused on[4]:

- **Integration –** gender equality must be considered as an integral part of NATO policies, programmes and projects guided by effective gender mainstreaming practices;
- **Inclusion –** promoting an increased representation of women across NATO and in the armed forces of member states and partner nations in order to enhance operational effectiveness and mission success; through this strategy, NATO seeks to raise women participation within all Alliance tasks, both military and civilian, and at all hierarchical levels;
- **Integrity –** systemic inequalities are approached with the purpose of assuring an objective and equitable treatment to all male and female staff of the Alliance; as a consequence, enhancing accountability with the intent to increase awareness and implementation of the WPS agenda in accordance with international frameworks becomes a priority.

Gender equality must be considered as an integral part of NATO policies, programmes and projects guided by effective gender mainstreaming practices.

Essentially, through this visionary policy, next to its allies and partner nations, NATO aims to integrate gender perspective

[1] ***, NATO, "NATO/EAPC policy for implementing UNSCR 1325 on Women, Peace and Security, and related Resolutions", 2011, retrieved on 11 April 2019, available at https://www.nato.int/cps/en/natohq/official_texts_76395.htm?selectedLocale=en

[2] Available at https://www.wikigender.org/wiki/un-security-council-resolution-1325-2/, retrieved on 17 April 2019.

[3] ***, NATO, "Comprehensive Report on the NATO/EAPC Policy on the Implementation of UNSCR 1325 on Women, Peace and Security and Related Resolutions", "Section 5 – Towards Implementation", 2010, retrieved on 12 April 2019, available at https://www.nato.int/cps/en/natolive/official_texts_68578.htm.

[4] ***, NATO, "NATO/EAPC Women, Peace and Security Policy and Action Plan", 2018, p. 7, retrieved on 12 April 2019, available at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_09/20180920_180920-WPS-Action-Plan-2018.pdf

ROMANIAN MILITARY THINKING

at the level of each of the three core tasks of the Alliance, collective defence, crisis management and security though cooperation, and to set the premises of an organisation capable to react in a prompt and adapted manner to the challenges posed by the reality of the contemporary security environment.

The **NATO/EAPC Action Plan** represents the main document regarding the above-mentioned policy setting into practice, both being designed to function in tandem. The actions described within the Plan derive from the "Women, Peace and Security" agenda issued by the United Nations and they are harmonised, in terms of a global and unitary implementation, with all the other international provisions that form the legal framework regarding women rights and gender equality. The Plan is revised on a bi-annual basis, thus providing all responsible NATO structures involved within the advancement of UNSCR 1325 with a real time image of the way in which the activities comprised in the Plan tailor to meet the requests of the security environment. Furthermore, the objectives and the courses of action are evaluated by measuring their degree of fulfilment through periodical reports. In the NATO/EAPC Action Plan, valid for 2018 – 2020, a series of *objectives of interest*[5] prevail, which are capable through their universality to generate notable results regarding the international security and defence domain.

The NATO/EAPC Action Plan represents the main document regarding the above-mentioned policy setting into practice, both being designed to function in tandem. The actions described within the Plan derive from the "Women, Peace and Security" agenda issued by the United Nations and they are harmonised, in terms of a global and unitary implementation, with all the other international provisions that form the legal framework regarding women rights and gender equality.

From the integration perspective:

- Strengthening the institutional framework;
- Enhancing engagement, cooperation and coordination with other international organisations on WPS;
- Strengthening Civil Society/NATO cooperation through regular engagement;
- NATO-led activities, operations and missions are enhanced through the integration of gender perspectives;
- Mechanisms to encourage exchanging information and sharing best practices are strengthened;
- Gender perspectives are addressed in efforts and strategies related to Emerging Security Challenges;
- Gender perspectives are included in Defence Planning Process;

From the inclusion perspective:

- Greater gender balance is in place across NATO;
- Improving the understanding by NATO civilian and military staff of the practical implications and benefits of the WPS agenda;
- Gender perspectives are integrated in NATO's defence and security related capacity building efforts;

From the integrity perspective:

- Specific measures to prevent sexual exploitation and abuse (SEA) in NATO led operations and missions are enforced;
- Measures to prevent and respond to sexual harassment at NATO are improved;
- Enhancing protection of women and girls from human trafficking through the updated NATO Policy on Combating Trafficking in Human Beings;

From the public diplomacy perspective:

- Increasing visibility of NATO's Women, Peace and Security agenda and of the efforts undertaken on the implementation;

Regarding monitoring and evaluation:

- Enhancing accountability is in line with monitoring and evaluation mechanisms.

romania2019.eu

The Bi-Strategic Command Directive 40-1 was adopted in 2009, at the proposal of the Strategic Commanders, and it serves as a core document for integrating gender provisions from UNSCR 1325 and its connecting resolutions into NATO operational terms[6]. It serves as a fundamental document in applying *"Women, Peace and Security"* dispositions within the NATO military component.

The Bi-Strategic Command Directive 40-1 was adopted in 2009, at the proposal of the Strategic Commanders, and it serves as a core document for integrating gender provisions from UNSCR 1325 and its connecting resolutions into NATO operational terms. It serves as a fundamental document in applying "Women, Peace and Security" dispositions within the NATO military component.

The Directive acknowledges the premises that support the entire case for the disproportionate impact of war upon male and female population that is forced to face major roles and statuses shifts as a consequence of them belonging to certain societies. Furthermore, it stipulates that gender perspective integration exhibits positive outcome for operational effectiveness due to the unique and complex way the security environment is interpreted, but also due to the various contributions brought to this floor by the human resource,

[5] ***, NATO, "NATO/EAPC Women, Peace and Security Policy and Action Plan", 2018, pp. 19-25, retrieved on 12 April 2019, available at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_09/20180920_180920-WPS-Action-Plan-2018.pdf

[6] ***, NATO, Bi-SC Directive 40-1, *"Integrating UNSCR 1325 and Gender Perspectives in the NATO Command Structure"*, 2017, retrieved on 15 April 2019, available at https://www.act.nato.int/images/stories/structure/genderadvisor/nu0761.pdf

all these being possible in the context of working in mixed teams. Thus, it highlights the importance of involving females in all stages of conflict and crisis development, as active promoters of sustainable peace.

The way the Directive is organised reveals the internally oriented component of this document, one that approaches processes such as recruitment, training and expertise for the military side of NATO and its partner and member states, from a perspective that is fully consistent with the international provisions regarding gender equality. Thus, this document introduces a new analysis instrument that is found in the process of planning and conducting operations and that implies added prospects upon situational awareness, force generation, conduct of operations and reporting. The Directive also establishes the subordination and the characteristics of the Gender Adviser (GENAD) and the Gender Focal Point (GFP) positions[7]. Although essentially the activities of these two types of functions correspond, there are still some characteristics that specifically refine each position.

- *Gender Adviser (GENAD)* – strategic level – staff appointed to permanent positions that are member of the advisory commanders group and are directly subordinated to the top decision-making persons. The level of their training and expertise needs to be advanced as they provide advice on the timely and proper gender mainstreaming and the integration of gender perspective including, but not limited to, operations/missions, crisis/conflict analysis, concepts, doctrine, procedures and education and training.
- *Gender Focal Point (GFP)* – operational and tactical level – are COS nominated personnel and dual-hatted within HQs, divisions/directorates and branches having received specific training on gender perspective and the implementation of UNSCR 1325 and related Resolutions; GFPs facilitate gender mainstreaming into the daily work, by supporting and enabling a professional and functional network throughout the HQ and military units, in order to maintain dialogue, liaison and coordination on the integration of gender perspectives.

The Bi-Strategic Directive 40-1 also makes reference to the standards of behaviour regarding prevention and response in cases

The way the Directive is organised reveals the internally oriented component of this document, one that approaches processes such as recruitment, training and expertise for the military side of NATO and its partner and member states, from a perspective that is fully consistent with the international provisions regarding gender equality. Thus, this document introduces a new analysis instrument that is found in the process of planning and conducting operations and that implies added prospects upon situational awareness, force generation, conduct of operations and reporting.

[7] *Ibid*, Chapter 5, p. 19, available at https://www.act.nato.int/images/stories/structure/genderadvisor/nu0761.pdf

of sexual violence based on gender differences that occur during conflict development, and especially during military interventions. In this regard, the NATO Code of Conduct remains of reference, as it establishes the personal and professional standards to which the military staff have to comply within the Alliance. This set of standards is intended to protect the efficiency and credibility of the organisation, at the same time, providing the troops fighting under the NATO aegis with the necessary legitimacy for fulfilling their national or international missions. On the contrary, not complying with the Code of Conduct may generate an additional source of insecurity, with negative effects on the military personnel or on the mission conduct, a situation that involves immediate actions to be taken by the commanders. Depending on the degree of gravity of the act, the sanction may be decided under administrative, disciplinary or penal provisions of the law.

NATO specific mechanisms for gender mainstreaming

UNSCR 1325 Resolution, together with all the other dispositions on the *"Women, Peace and Security"* agenda, are currently fully integrated within the Alliance, covering a large spectrum of missions and operations, whose evolution determines the degree and the pace of this agenda's advancement. As an extremely efficient security provider, NATO has succeeded in internationally imposing itself as the main defender and guarantor of gender equality, especially in extremely vulnerable situations.

With the help of the UNSCR 1325 attached legislation and with the new implementation mechanisms, the number of women participating in missions carried on in different theatres of operations is increasing, simultaneously with the growing percentage of women that apply for military carrier within the armed forces of member states. Encouraging nations to give up low admittance quotas for women in relation to the military systems or the interdiction for them to join certain combat specialties and branches, as well as the unitary quotation of the fitness tests have resulted, for the past 20 years, in evolutions regarding recruiting and maintaining the human resource, based solely on one selection criterion, which is professionalism. Using highly specialised NATO structures for gender mainstreaming, the armed forces have received the necessary training in order to be capable of transforming this domain into a true military asset. The terrorist threat, associated

The Bi-Strategic Directive 40-1 also makes reference to the standards of behaviour regarding prevention and response in cases of sexual violence based on gender differences that occur during conflict development, and especially during military interventions. In this regard, the NATO Code of Conduct remains of reference, as it establishes the personal and professional standards to which the military staff have to comply within the Alliance.

ROMANIAN MILITARY THINKING

with the Muslim world, has validated in a more precise manner the importance of enhancing these types of capabilities, as the specificity of the local population deriving from a social, religious or customary perspective imposed the presence of military women in the missions carried on the theatres of operations.

A good example, among many others, may be the ISAF mission developed in Afghanistan, during which a series of enablers regarding gender mainstreaming have led to better awareness and analysis of the operational context, providing essential information for an efficient, much better oriented and in-depth military approach, all with a minimum involvement of other resources. The NATO Regional Commands have thus used:

A good example, among many others, may be the ISAF mission developed in Afghanistan, during which a series of enablers regarding gender mainstreaming have led to better awareness and analysis of the operational context, providing essential information for an efficient, much better oriented and in-depth military approach, all with a minimum involvement of other resources.

- Female Engagement Teams (FET) – meant to gather information and provide analysis on the atmospherics regarding the host nation, which are required in the operations planning process; they have been deployed, based on their mandate, as part of intelligence structures or as civil and military cooperation units, as it was for the Romanian teams;
- Cultural Support Teams (CST) – designed to support special operations by shaping them in a culturally sensitive manner, and by respecting the role and the status of women within the Muslim society;
- Foreign Area Specialists (FAS) – deployed as a tool linked to the information, communication operations and PsyOps; they are responsible for meeting influential women in the area of operations, with the purpose of revealing the networks and decision-making mechanisms from the female population perspective.

The use of this type of expert teams has imposed a new pace for mission development, by highlighting the human security component as well as by integrating additional complex perspectives in the operational environment. Following the results acquired in terms of intelligence gathering and positive impact of integrated humanitarian assistance actions, as well as long-term project development initiated for the local female host population, it resulted that the efforts regarding peace and security enforcement and keeping is much more sustainable when women become equal partners of men in conflict prevention and post-conflict reconstruction.

romania2019.eu

Once assuming the lessons identified and learned within the theatres of operations, in missions such as ISAF (International Security Assistance Force), NTM – A (NATO Training Mission Afghanistan) or KFOR (Kosovo Force), NATO has managed to improve its working mechanisms regarding gender mainstreaming at the level of the armed forces. In parallel, it succeed in raising awareness of troops on matters regarding women involvement in security and defence, a fact that generated reform across the system of recruitment, teaching/training, and human resources management during missions. At present, according to the annual reports send by the member nations prior to the Annual Conference of the NATO Committee on Gender Perspectives (NCGP), an evaluation of the indicators attesting active and continuous involvement of the Alliance in the advancement of "Women, Peace and Security" agenda is facilitated. Consequently, for the women representation within the armed forces of the NATO member states, a general and also particular ascendant tendency may be observed, in regard to applying for different branches, military specialties or deployment to various theatres of operations:

- 10.8% the medium percentage of female representation across the NATO armed forces[8];
- 6.4% the medium percentage of female representation within international missions carried under the NATO aegis[9].

Female repartition on armed forces categories at the level of the Alliance's member states is the following[10]: Land Forces – 48%; Air Forces – 20%; Naval Forces – 13.7%; Other – 20%.

Repartition depending on the top five military specialties chosen by NATO active military female staff[11]: Other – 24.7%; Medical services – 23.5%; Logistics – 10.5%; Infantry – 10.5%; Communications – 6.5%.

The annual national reports represent the proof that NATO permanently evolves and adapts itself to the international requirements

Female repartition on armed forces categories at the level of the Alliance's member states is the following: Land Forces – 48%; Air Forces – 20%; Naval Forces – 13.7%; Other – 20%. Repartition depending on the top five military specialties chosen by NATO active military female staff: Other – 24.7%; Medical services – 23.5%; Logistics -10.5%; Infantry – 10.5%; Communications – 6.5%.

[8] ***, NATO, *NATO Annual Review on Gender in Military: Progress Made in Policies, Participation and Operational Planning*, retrieved on 17 April 2019, available at https://www.nato.int/cps/en/natohq/news_140013.htm.

[9] *Ibid.*

[10] ***, NATO, *Summary of the National Reports of NATO Member and Partner Nations to the NATO Committee on Gender Perspectives*, Brussels, 2016, p. 23, retrieved on 17 April 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_01/1801-2016-Summary-NR-to-NCGP.pdf.

[11] *Ibid*, p. 24.

regarding the assurance of equal opportunities within professional environment, currently having equal admittance standards in the field of security and defence, and also supporting a policy of equilibrating the work-life balance, all with the purpose of advertising, motivating and raising retention in the military system for the most talented human resource.

The implementation of *"Women, Peace and Security"* Resolutions is a process developed at various levels of the divisions and governing bodies within NATO Headquarters as well as in the Strategic Commands. Together, these entities are responsible for monitoring and reporting the progress made by the Alliance. For this purpose, a *"Women, Peace and Security"* Task Force was established under the guidance and responsibility of the Special Representative for *"Women, Peace and Security"*. The NATO mechanisms that give impetus to the gender perspective mainstreaming making the Alliance an international hub for this domain are[12]:

- The Secretary General's Special Representative for Women, Peace and Security serves as the high-level focal point on all aspects of NATO's gender/Women, Peace and Security – related work. This position was created in 2012 and made permanent from September 2014;
- A task force bringing together civilian and military staff across NATO Headquarters;
- A gender adviser in the International Military Staff and an advisory committee of experts (NATO Committee on Gender Perspectives) on the military side, tasked with promoting gender mainstreaming in the design and implementation, monitoring and evaluation of policies, programmes and military operations;
- A working group led by Allied Command Operations to assess means to further incorporate the UNSCRs on *"Women, Peace and Security"* into operational planning and execution;
- Gender advisers deployed at different levels of NATO's military command structure, including operational headquarters;
- A number of relevant committees that develop and review specific and overall policy;
- The NATO Science for Peace and Security (SPS) Programme promotes actual, practical cooperation on gender-related issues among NATO member and partner countries, through collaborative multi-year projects, training courses, study institutes and workshops;
- The Consultative Panel of Civil Society (CSAP), to support and guide the work of *"Women, Peace and Security"* within NATO and advise on the integration of gender perspectives into NATO's core tasks.

The implementation of "Women, Peace and Security" Resolutions is a process developed at various levels of the divisions and governing bodies within NATO Headquarters as well as in the Strategic Commands. Together, these entities are responsible for monitoring and reporting the progress made by the Alliance. For this purpose, a "Women, Peace and Security" Task Force was established under the guidance and responsibility of the Special Representative for "Women, Peace and Security".

[12] Retrieved on 19 April 2019, available at https://www.nato.int/cps/en/natohq/topics_91091.htm.

Conclusion

Gender represents a dimension of personal life, social relations and culture. Across time, it has been an arena within which complex practical problems have been confronted in terms of justice, identity and even survival.

Gender is also a controversial subject that was treated as a myth surrounded by countless biases. Latest years research in human sciences have dismantled a lot of those biases, by bringing this subject close to the military and political concerns, as a key element of generating evolution in the social domain, and respectively in the security and defence domain.

Armed conflicts have always exerted a tremendous and different impact upon population depending on several coordinates, such as gender, ethnicity, or social class. Contemporary conflicts, generated by the hybrid tactics used during their development, prove through their effects that gender issues need to be taken into consideration as a relevant dimension that influences security. The adoption of the UNSCR 1325 family of Resolutions is an essential landmark of gender perspectives integration within the military operations, in post-conflict resolutions and also in the peace negotiations.

World-wide security providers, and especially NATO, have exploited this tendency and transformed it, for their benefit, into a capability retrieved at all levels, strategic, operational and tactical, a capability that uses the *"Women, Peace and Security"* provisions to provide the troops that are deployed internationally with the mandate and the interoperable means necessary for successful mission accomplishment. NATO has gradually transformed into a true centre

Armed conflicts have always exercised a tremendous and different impact upon population depending on several coordinates, such as gender, ethnicity, or social class. Contemporary conflicts, generated by the hybrid tactics used during their development, prove through their effects that gender issues need to be taken into consideration as a relevant dimension that influences security. The adoption of the UNSCR 1325 family of Resolutions is an essential landmark of gender perspectives integration within the military operations, in post-conflict resolutions and also in the peace negotiations.

ROMANIAN MILITARY THINKING

Being an international hub for gender mainstreaming, NATO will continue to actively support the education and the specialised training of troops by respecting gender equality and adapting its operational design to the international legal framework that is in force, on this theme. In this context, the organisation remains a true source of inspiration regarding the consistency of the lessons observed and learned, as well as the creative ideas involved in the process of implementing gender perspective within the complex security and defence domain, a domain on whose stability the prevalence of future generations and the faith of humanity depend.

of excellence in promoting and applying the gender equality dispositions, not as an obligation imposed by social reality, but as an important aspect of using full human capital with a minimum of resources, within an original operational architecture. The stake of the success has consisted in approaching all gender differences as strong points and also in exploiting them in intelligent decisional processes, based on diversity, with the purpose of spotting solutions and brand new opportunities that are viable for solving acute global issues.

Being an international hub for gender mainstreaming, NATO will continue to actively support the education and the specialised training of troops by respecting gender equality and adapting its operational design to the international legal framework that is in force, on this theme. In this context, the organisation remains a true source of inspiration regarding the consistency of the lessons observed and learned, as well as the creative ideas involved in the process of implementing gender perspective within the complex security and defence domain, a domain on whose stability the prevalence of future generations and the faith of humanity depend.

Diversity is not a self-generated phenomenon. NATO excellence in gender perspective implementation resides in the fact that the organisation has understood that diversity is the product of political will manifestation and good intentions appliance, all maintaining the momentum. In this regard, we refer not only to fast adoption of laws, political frameworks or in force directives, but also to the necessity of promoting those champions of change that are capable of creating an inclusive environment, at all levels of the organisation. This context was and still is profoundly true for NATO, given the fact that even though, traditionally, defence and security have been the privilege of men, currently maintaining a gender balance and incorporating diversity define de essence of individual and collective efforts sustained by the Alliance on the coordinates of its three core tasks, respectively crisis management, security through cooperation and collective defence.

BIBLIOGRAPHY

1. ***, *NATO Annual National Reports*, published on https ://www.nato.int.
2. ***, North Atlantic Treaty Organization*, Bi-SC Directive 40-1, Integrating UNSCR 1325 and Gender Perspectives in the NATO Command Structure*, Brussels, 2017.
3. ***, North Atlantic Treaty Organization*, Comprehensive Report on the NATO/EAPC Policy on the Implementation of UNSCR 1325 on Women, Peace and Security and Related Resolutions*, Brussels, 2010.
4. ***, North Atlantic Treaty Organization, *NATO/EAPC Policy on Women, Peace and Security*, Brussels, 2018.
5. ***, North Atlantic Treaty Organization, *NATO/EAPC Women, Peace and Security Action Plan*, Brussels, 2018.
6. ***, North Atlantic Treaty Organization, *Summary of the National Reports of NATO Member and Partner Nations to the NATO Committee on Gender Perspectives*, Brussels, 2016.
7. Carol Cohn, *Women and Wars*, Polity Press, London, 2018.
8. Claire Duncanson, *Gender and Peacebuilding*, Polity Press, London, 2016.
9. Theodora-Ismene Gizelis, Louise Olsson, *Gender, Peace and Security – Implementing UN Security Council Resolution 1325*, London, Routledge, 2016.
10. Helene Lackenbauer, Richard Langlais, *Review of the Practical Implications of UNSCR 1325 for the Conduct of NATO-led Operations and Missions*, Brussels, 2013.
11. Laura Sjoberg, *Gender, War and Conflict*, Polity Press, London, 2014.

romania2019.eu

CASE STUDY ON THE POTENTIAL APPLICATION OF SERIOUS GAMING IN THE AREA OF EUROPEAN DEFENCE

Nikolay PAVLOV
Stefan HADJITODOROV
Atanas RADEV
Martin SOKOLOV
Centre for National Security and Defence Research at the Bulgarian Academy of Sciences

The paper presents a case study of the potential application of serious gaming in the area of European Defence. In the last years game technology has been successfully applied to enhance capabilities in many areas, including in the training of peacekeeping personnel. The role of serious game technology for EU Defence has not been sufficiently explored. The research hypothesis is that serious gaming could serve as a tool for an in-depth study and foresight of alternative scenarios for the future development of EU Defence.

Keywords: Serious gaming, European defence, Common Security and Defence Policy (CSDP).

romania2019.eu

Introduction

The paper seeks to explore the potential application of serious gaming in EU Defence. Serious gaming is considered as a global revolution in interactive 3D technology that promises to develop intuitive, affordable, accessible and familiar training environments for a wide range of educational and training applications, from medicine and healthcare to defence training[1]. The primary ambition of serious gaming – to achieve immersive experiences in lifelike environments populated with *"avatars"* representing real human participants from across the world –is closer today than ever before. Nowadays, personal computers, game consoles (e.g. Xbox, PlayStation or GameCube) and the Internet provide easy access to different kinds of solutions for single and multi-players games, starting from complete virtual worlds (e.g. Second Life), continuing with role games (e.g. World Warcraft) and ending with military tactical first-person shooters (e.g. Call of Duty)[2]. In this context the paper will explore the potential of serious gaming for enhancing EU Defence and, specifically, the EU's Common Security and Defence Policy (CSDP). It builds upon the latest institutional developments in CSDP such as the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF).

Serious gaming is considered as a global revolution in interactive 3D technology that promises to develop intuitive, affordable, accessible and familiar training environments for a wide range of educational and training applications, from medicine and healthcare to defence training.

The paper considers two types of games – finite and infinite. The former is based on known players, fixed rules, and agreed upon objectives; the latter consists of known and unknown players, modifiable rules, and the objective itself is to keep the game going. Notable examples of infinite games are the Cold War, pertaining to war and security, and business and economics in peaceful periods. A finite game continues until the objectives are reached, whereas an infinite game ends for an actor or player when they are forced to quit,

[1] Robert Stone, *Game on! The Role of Human Factors in Serious Gaming for Defence Medicine and Other Real-time Training Applications*, in Conference Proceedings from Conference *People and Systems – Who Are We Designing For*, 2005. The IEE and MOD HFI DTC Symposium.

[2] Zlatogor Minchev, *EEG Spectral Analysis in Serious Gaming: An Ad Hoc Experimental Application*, BIOautomation, 2009, 13 (4), pp. 79-88.

ROMANIAN MILITARY THINKING

for example the Soviet Union at the end of the Cold War. Thus, it is vital for a player to understand in what type of game he is participating, as if he is wrong, this may lead to miscalculation.

The EU, however, is a complex actor – a Union that consists of independent sovereign states that have willingly delegated certain authority and decision-making power to a centralised authority, i.e. Brussels, in exchange for shared prosperity, security and other overall gains. This will allow the EU to participate in both games at the same time – finite internally and infinite internationally.

The EU is a complex actor – a Union that consists of independent sovereign states that have willingly delegated certain authority and decision-making power to a centralised authority, i.e. Brussels, in exchange for shared prosperity, security and other overall gains. This will allow the EU to participate in both games at the same time – finite internally and infinite internationally.

The EU has now existed for over 7 decades. In this period, it has encountered various actors and threats – from the Soviet Union to Russia, non-state actors, and the rise of China. Among its goals are to promote democracy, peace, and prosperity. Such objectives work over extended periods of time and, when and if achieved, this will not end the game for the EU. Therefore, Brussels' goal needs to be to perpetuate the game on the international level. It is also to be noted that the EU has encountered changes in the rules. Most notably and most recently, this has been evidenced in the tariffs imposed by Washington. This also signals the necessity of adaptability.

Internally, however, the EU is faced with a predominantly finite game – the main players are the member-states and the bodies of the Union, there are fixed rules and there are penalties involved if they are broken (consider Poland and Hungary), and the semi-finite objective is to enhance cooperation, the rule of law, equality, democracy, and promote prosperity.

EU Defence Scenarios

Based on observations of the EU's institutional developments in the years after the Lisbon Treaty several alternative scenarios for the development of EU Defence could be elaborated. The scenarios further elaborate the three scenarios set out in the Reflection Paper on the Future of European Defence[3] but are not limited to those *"official scenarios"*. In addition, scenario development draws on the more general scenarios in the White Paper on the Future of Europe[4],

[3] *Reflection Paper on the Future of European Defence*, European Commission COM(2017) 315 of 7 June 2017.

[4] *White Paper on the Future of Europe*. Reflections and scenarios for the EU27 by 2025 (COM (2017) 2025 final), Brussels, 1 March 2017.

political statements and *"visions"* for the EU[5], empirical data and lessons learned from the 20-year-old CSDP[6]. As a minimum five scenarios could be outlined, as follows:

romania2019.eu

1) Security and defence cooperation

In this scenario the level of defence integration is low, whereas multilateral defence cooperation remains mostly on paper. This *"pessimistic"* scenario corresponds to the scenario *"Nothing but the single market"* in the White Paper, whereas the EU is gradually re-centred on the Single market. EU Member States demonstrate preference to bilateral defence arrangements and to great extent pursue independent defence and security policies. The Union is able to mobilise support for peacekeeping missions and operations by *"coalitions of the willing"* only on an *ad hoc* basis. Sporadic initiatives for greater defence cooperation could be launched but will not amount to much.

In the scenario related to defence cooperation, the level of defence integration is low, multilateral defence cooperation remaining mostly on paper. This "pessimistic" scenario corresponds to the scenario "Nothing but the single market" in the White Paper, whereas the EU is gradually re-centred on the Single market. EU Member States demonstrate preference to bilateral defence arrangements and to great extent pursue independent defence and security policies.

2) Shared security and defence

Medium level of defence integration, whereas several *"core"* countries conduct defence R&D, develop, pool and share equipment. This scenario corresponds to the White Paper scenario *"Those who want more do more"*, whereas certain Member States do more together in specific policy areas. In this scenario the number of Member States (10-12) which actively participate in defence cooperation initiatives is limited. Only a group of countries deepen defence cooperation focusing on military coordination and joint equipment. The Union is able to organise CSDP missions and operations only in the medium-term (1-2 years) after the breakout of a crisis.

As a sub-scenario the *"core group"* could establish closer defence cooperation with selected EU Member States and non-EU countries. A case in point is the European Intervention Initiative (E2I) which has been recently spearheaded by France and which includes 9 Western European EU Member States plus the United Kingdom.

[5] See for example: Hans Kundnani, *Competing Visions of Europe Are Threatening to Tear the Union Apart,The Guardian,* 1 July 2018.

[6] For a recent study of the CSDP, see: Michael Smith, *Europe's Common Security and Defence Policy: Capacity-building, Experiential Learning and Institutional Change*, Cambridge: Cambridge University Press, 2017.

ROMANIAN MILITARY THINKING

3) Common defence and security

High level of integration of EU Member States' defence capabilities and development of joint equipment. This scenario corresponds to the White Paper scenario *"Doing much more together"*, whereas a European Defence Union is created in full complementarity with NATO. In this scenario most of the EU Member States will actively participate in the process of developing common EU defence capabilities potentially with a view towards building-up European Armed Forces. The Union is an autonomous *liberal* global player on the international arena which speaks with one voice on all foreign policy issues. Initiatives such as PESCO, EDF and EDIDP (European Defence Industrial Development Programme) are fully developed and operational. This is the most optimistic scenario developed by the EU bureaucracy.

The proposed "Europe First" scenario draws upon the general European Far Right/Nationalist idea of "Fortress Europe" interpreted in identitarian terms as Christian Europe of sovereign nation-states. A good starting point is the Austrian Presidency of the Council of the EU as the allegedly far-right Freedom party plays a prominent role in Austria's government.

4) *"Europe First"* scenario

The proposed *"Europe First"* scenario draws upon the general European Far Right/Nationalist idea of *"Fortress Europe"* interpreted in identitarian terms as Christian Europe of sovereign nation-states. A good starting point is the former Austrian Presidency of the Council of the EU as the allegedly far-right Freedom party plays a prominent role in Austria's government. The motto of the 2018 Austrian Presidency *"A Europe that protects"* is clearly directed at fighting illegal migration and this seems to be the common denominator and the top priority for all European Radical Right parties. It could be expected that in the event of stronger and more coherent presence of the European Radical Right in the European Parliament after May 2019 the fight against illegal migration could be streamlined under the EU's Common Security and Defence Policy which is likely to encompass also border management of the Union. That would entail a great institutional reshuffle in many EU bodies such as FRONTEX, the European External Action Service (EEAS) and others. In this scenario the establishment of Migration centres outside EU borders – as proposed by the Austrian Chancellor Sebastian Kurz[7]–could be expected. Setting-up and managing Migration centres outside the EU could become some of the major tasks for CSDP missions and operations. The so-called liberal peace concept – which

[7] *Austria Backs Migration Centers in Non-EU Countries*, Politico 11/07/2018, https://www.politico.eu/article/sebastian-kurz-austria-backs-migration-centers-in-non-eu-countries/

has for long dominated EU's conflict prevention and peacebuilding, at least in theory – would be side-lined.

Given the historically close links between nationalism and the military ethos it is very likely that the level of ambition for defence-industrial and R&T (research and technology) cooperation in the *"Europe First"* scenario would be high. Of course, enhanced defence integration would be possible only under the leadership of the *"big two"* EU Member States (remaining) – Germany and France, or at least one of them. It is highly probable that the implementation of defence cooperation initiatives such as the newly established Permanent Structured Cooperation (PESCO) and the European Defence Fund would be challenging.

One of the most geopolitically charged issues in the *"Europe First"* scenario would be the relations of the EU with the US and Russia. As in European societies extremely divergent views on the relations with those global powers co-exist one could argue that the EU should stay neutral towards both the US and Russia and to focus on the effective development of the EU's strategic autonomy. However, it is more realistic to expect that a great controversy, if not a split within the European Radical Right, could be expected over the EU's relations with the US and Russia.

romania2019.eu

One of the most geopolitically charged issues in the "Europe First" scenario would be the relations of the EU with the US and Russia. As in European societies extremely divergent views on the relations with those global powers co-exist one could argue that the EU should stay neutral towards both the US and Russia and to focus on the effective development of the EU's strategic autonomy. However, it is more realistic to expect that a great controversy, if not a split within the European Radical Right, could be expected over the EU's relations with the US and Russia.

5) Setting-up a Euro-Atlantic Union

In this scenario NATO and EU would be unified into a common federal supranational structure. This is a futuristic scenario for a new social, political and military union based on the *"former"* NATO and EU countries on the territory of Europe. As a result of the withdrawal of the US from NATO the former European allies are becoming politically and militarily weak. Due to the formation of an Anti-European alliance in the Middle East and Asia and the sustained migrant flows the former NATO and EU member states establish a highly integrated Euro-Atlantic Union spanning on two continents which develops common Euro-Atlantic defence forces.

Such a scenario could be based on the Transatlantic Trade and Investment Partnership (TTIP), which aims to bring the two biggest economies together – the US and the EU. While negotiations have been halted indefinitely since 2016, will to resume negotiations has been expressed by German Chancellor Angela Merkel on 27 June 2017. The three focus areas are market access, specific regulation, and broader

ROMANIAN MILITARY THINKING

rules and principles and modes of co-operation[8]. Progress of the TTIP can and should be considered a stepping stone for deepening cooperation between the US and the EU. This scenario speculates that together with the economic partnership, US-EU cooperation could also be translated to the defence and security domain.

It should be noted that the scenarios cannot be considered as absolutely *"pure"* and refined reference subjects. In the highly complex and volatile international security environment some of these scenarios could overlap and *"mixed"* scenarios could take place *"on the ground"* in reality. Of course, the number of scenarios could be increased by the force of imagination and the multiplying effect of sub-scenarios. In order to make a meaningful scientific contribution the paper and the proposed game concept will focus on the above-described five basic scenarios for the development of European Defence.

The scenarios cannot be considered as absolutely "pure" and refined reference subjects. In the highly complex and volatile international security environment some of these scenarios could overlap and "mixed" scenarios could take place "on the ground" in reality. Of course, the number of scenarios could be increased by the force of imagination and the multiplying effect of sub-scenarios. In order to make a meaningful scientific contribution the paper and the proposed game concept will focus on the above-described five basic scenarios for the development of European Defence.

"EU Defence" Game Concept

So far, the potential application of serious gaming in EU Defence has been under explored. With the exception of some *ad hoc* wargaming exercises (mostly cyber security-related) serious gaming has not been utilised to enhance EU Defence. This paper's contribution in this respect is a preliminary serious game concept which is tailored specifically for playing EU Defence scenarios.

The *"EU Defence"* game concept includes the core idea, the game *"story"*, the main characters (nations and international organisations) and the target audiences (end-users). The main features of the alternative scenarios are as follows:

- Geopolitical balance of powers;
- Resources;
- Territory / Maps;
- Conflicts;
- Levels of the game.

The Game concept will be implemented in a seven-step iterative process, as follows:

I. Defining the scenario.

1. Purpose of the scenario.

- Generating a range of options to consider depending on what the external environment might look like in the future.

[8] *State of Play of TTIP Negotiations ahead of the 6th Round of Negotiations*, European Commission DG Trade, 11 July 2014, retrieved on 30 July 2018.

romania2019.eu

2. Timeframe.

- Long-term planning technique (for example 3, 5, 10 years into the future).

3. Focus.

- Addressing the intersection to single or several events (trends/players, competitors, regulations and regulators etc.).

II. Assign players to teams.

1. Defining the players and forming the teams.

2. 3rd party (neutral) players with no key features.

III. Describing current conditions (context) in fields like resources, environment and defence capabilities.

1. Using GIS.

- Terrain builder (mountains, resources, waters etc.), realistic layers (rivers, canyons, nature etc.).

2. Key players' capabilities and natural advantages and weak sites.

IV. Developing strategy.

V. Testing scenario.

VI. Wrapping up the results.

VII. Repeating step III, IV and V until the desired outcome.

Example for the Implementation of the Game Concept:

The "EU Defence" game concept includes the core idea, the game "story", the main characters (nations and international organisations) and the target audiences (end-users). The main features of the alternative scenarios are as follows: Geopolitical balance of powers; Resources; Territory/Maps; Conflicts; Levels of the game.

Table 1

Game Mode			
Defining scenario	Setting-up a Euro-Atlantic Union		
Purpose of the scenario	Development of an alternative foresight scenario for the development of EU Defence under a wider Euro-Atlantic geopolitical framework.		
Timeframe	2030-2040		
Focus	Defence capabilities development		
Assigning teams			
Defining players	Euro-Atlantic Union	Eurasian Union	New Islamic State/Suni Muslim Khalifate
3rd party or neutral players	Countries like Switzerland, Israel, Australia etc.	Japan, China	Iran (Shia Muslim community)

ROMANIAN MILITARY THINKING

Game Mode			
Current conditions for the defined players			
Nature	NATO and EU are unified into a common federal supranational structure. The geopolitical nature is sea-oriented based on the Union's political geography.	The Eurasian Union is developed as a new form of the Russian empire. The geopolitical nature is land-based rooted in the traditions of the Steppe empires of the past and the geopolitical legacy of the Soviet Union.	A new militant Islamic state is established in the Near East with the ambition to pursue jihad and to destroy the infidels.
Terrain	Miscellaneous, geographically determined.	Miscellaneous, geographically determined.	Mostly half-desert terrain.
Resources	Sufficient but diminishing resources.	Sufficient but diminishing resources.	Limited resources.
Strategy and Capabilities			
Attack	Defence doctrine	Offensive doctrine	Asymmetrical/ Terrorist act-based doctrine
Defence	The whole spectrum of defence capabilities: Air Force, Navy, Land Force, Cyber and Nuclear	The whole spectrum of defence capabilities: Air Force, Navy, Land Force, Cyber and Nuclear	Mostly land forces and suicide bombers
Military	Political control over the Armed Forces	Military mode of organisation of the society	Religious-military symbiosis

Game Mode			
Advantages			
	More democratic international outlook	Political stability and ability for fast mobilisation	Radically alternative world-view
	State-of-the-art defence technologies	State-of-the-art defence technologies	Great demographic potential
Weaknesses			
	Internal infightings between far-left, far-right and sectarian groups	Human rights violations	Economic backwardness
			Intra-religious infightings

romania2019.eu

Conclusion

The paper explores the potential application of serious gaming in EU Defence in the context of the specific EU dichotomy between finite and infinite games. A set of alternative scenarios for the development of EU Defence is elaborated which could be played by serious game technology. The proposed preliminary *"EU Defence"* game concept demonstrates that the alternative scenarios have the necessary features for a prospective tailored-made serious game focused on EU defence.

The preliminary "EU Defence" game concept demonstrates that the alternative scenarios have the necessary features for a prospective tailored-made serious game focused on EU defence.

FUTURE COMMAND AND CONTROL OF ELECTRONIC WARFARE

Commander Malte von SPRECKELSEN
DEU N, NATO Joint Electronic Warfare Core Staff,
Chairman of the NATO Electronic Warfare Working Group (NEWWG)

Major Erik BAMFORD
Norwegian EW Centre, Co-Chair of the Command and Control of EW sub-group within the NEWWG

The article is based on the presentation of the scenario during NATO Joint ISR Trial Unified Vision 2018. A helicopter crashed due to a malfunction well within a contested area. The pilot was not able to transmit his last position prior to the crash, which resulted in initiating the contingency plans for personnel recovery in hostile-controlled areas. The eight minutes from the initial incident to the successful localisation and identification of the crew could be rated as a great achievement, although the software, tools and systems used to coordinate the search were not at all advanced or highly sophisticated, and information was manually moved between the different systems to overcome the lack of connectivity and interoperability. The example highlights NATO's need for new tools and functional services to ensure proper Command and Control (C2) of Electromagnetic Operations (EMO). Therefore, a project of the C2 of EW is presented, having as ultimate goal to achieve EMS superiority.

Keywords: Command and Control, Electromagnetic Operations, Electronic Warfare, Electromagnetic Spectrum, connectivity, interoperability.

Article originally featured in JAPCC Journal, Issue 28, 2019, https://www.japcc.org/future-command-and-control-of-electronic-warfare/

New Functional Services are on Their Way to Enhance NATO's Ability to Effectively Command and Control Electromagnetic Operations.

Introduction

During a NATO-led operation, a helicopter crashed due to a malfunction. The helicopter crashed well within a contested area. Unfortunately, the pilot was not able to transmit his last position prior to the crash. This event changed the daily routine within the NATO Combined Joint Task Force ELBONIA staff who immediately initiated the contingency plans for personnel recovery in hostile-controlled areas. Without loss of time, the Commander reviewed the latest known geolocation of the helicopter and made the rescue of the downed crew his top priority.

All available assets and sensors were tasked to search for, identify and geo-locate the downed crew within the defined search area. The chief of the Electronic Warfare Coordination Cell (EWCC)[1] tasked his available Electronic Warfare (EW) assets to focus on any electromagnetic emissions related to the crash by issuing an updated Emission of Interest (EOI) list. The updated EOI covered call sign, combat identification last recorded transmission (time/space) and emergency beacon search priorities. The radio frequencies for the downed pilot's personal AN/PRC-112[2] Survival Radio were uploaded via the Cooperative Electronic Support Measure Operations (CESMO)[3] Fusion Cell (CFC). Instantaneously all CESMO equipped assets received the updated EOI to sense for the requested frequencies. The basic concept of CESMO is to increase NATO-led formations' collective exploitation through the benefits of using multi-platform intercept data. The collected multi-platform intercept data is shared in near

During a NATO-led operation, a helicopter crashed due to a malfunction. The helicopter crashed well within a contested area. [...] This event changed the daily routine within the NATO Combined Joint Task Force ELBONIA staff who immediately initiated the contingency plans for personnel recovery in hostile-controlled areas.

[1] *AD 80-19 Directive* for an Electronic Warfare Coordination Cell.
[2] *AN/PRC-112* device offers synthesised radio in the VHF and UHF aircraft bands. It is a *PRC-112* modified to include a GPS receiver, allowing encrypted position information to be sent. Also has *COSPAS-SARSAT (Cosmicheskaya Sistema Poiska Avariynyh Sudov – Search and Rescue Satellite-Aided Tracking)* beacon.
[3] *NATO STANAG 4658.*

real-time and supports the need for rapid geo-location of targets/ EOI from different locations (altitude and azimuth) and orientations. Near real-time sharing enables rapid and accurate geo-location and the ability to defeat threats in a matter of seconds. It also provides the ability to geo-locate and link up with allied forces who find themselves beyond the reach of established command systems.

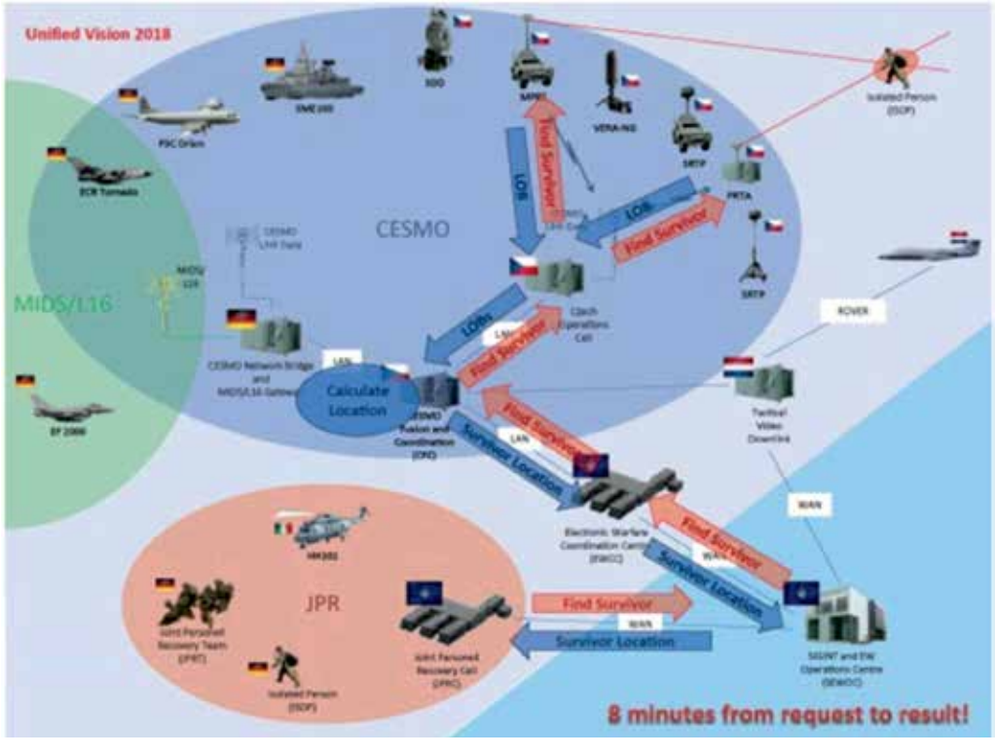


Figure 1: EW reporting chain at Unified Vision 2018 for the personnel recovery event.

The sensor network available on the day of the crash consisted of two Tornados[4], a P3C Orion[5] and some ground-based surveillance vehicles. Eight minutes after the crash the Chief of EWCC reported the triangulated position of the AN/PRC-112 to the operations centre. Immediately thereafter an available aircraft with video downlink capability was tasked to investigate the signal and verify the position.

[4] The *Panavia Tornado* is a family of twin-engine, variable-sweep wing multirole combat aircraft, which was jointly developed and manufactured by Italy, the United Kingdom, and West Germany. The Tornado IDS (interdictor/strike) version is employed as fighter-bomber.

[5] The *Lockheed P-3 Orion* is a four-engine turboprop anti-submarine and maritime surveillance aircraft developed for the United States Navy and introduced in the 1960s.

The helicopter and crew were found, and the rescue mission could proceed.

This scenario took place during NATO's Joint Intelligence, Surveillance and Reconnaissance (ISR) Trial *Unified Vision 2018*. The eight minutes from the initial incident to the successful localisation and identification of the crashed crew could be rated as a great achievement. However, it should be noted that the software, tools and systems used in the EWCC to coordinate the search in the spectrum were not at all advanced or highly sophisticated. The NATO Emitter Database (NEDB)[6], as a reference database, still runs its queries within a Microsoft® Access Database and the CFC was not connected with the rest of the NATO Trial Network. Information was manually moved between the different systems to overcome the lack of connectivity and interoperability. The current processing, including manual movement of information, requires additional staffing. This example highlights NATO's need for new tools and functional services to ensure proper Command and Control (C2) of Electromagnetic Operations (EMO). Command and Control (C2) of EW is designed to provide this.

The NATO Emitter Database (NEDB), as a reference database, still runs its queries within a Microsoft® Access Database and the CFC was not connected with the rest of the NATO Trial Network.

Figure 2: C2 of EW related word cloud.

Electromagnetic Operations

NATO forces are required to operate within an increasingly complex Electromagnetic Environment (EME)[7], which is defined as an operating environment[8] by NATO. Commanders are tasked to attain

[6] *STANAG 6009.*

[7] *MC 64/11 "NATO recognises the Electromagnetic Environment (EME) as an operating Environment".*

[8] According to NATO, *Operating Environment (OE)* is a composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander.

the level of superiority required to enable effective friendly forces' use of the EME while simultaneously exploiting, preventing or reducing the adversary forces' EME usage. EMO consists not only of EW but several other disciplines which operate in the EME, such as navigation warfare, spectrum management, and signal intelligence. As EW has evolved from isolated operations in the EME at the tactical level towards joint EMO at the strategic and operational level, EW remains the combat discipline of EMO.

NATO doctrine recognises that NATO operations are complicated by an increasingly congested and contested EME[9]. All modern forces conduct operations that depend on the use of the EME. The recognised need for military forces to have access to and utilise the EME creates vulnerabilities and opportunities for EW. Today's communication, sensing and guidance devices, whose function depends upon electromagnetic energy, are increasingly used both alone and in networked arrangements by civilian and military organisations[10].

Command and Control of Electronic Warfare – a Project

Command and Control of Electronic Warfare (C2 of EW) describes the development and implementation activities associated with the supporting functional services.

EMO demands a level of coordination and synchronisation which is impossible without specialised capabilities that support EME situational awareness, coordination and priority of actions.

Command and Control of Electronic Warfare (C2 of EW) describes the development and implementation activities associated with the supporting functional services.

The C2 of EW project will be implemented incrementally. The first increment will replace the legacy fielded NEDB as the foundational data provider for C2 of EW. The second increment should fulfil the Minimum Military Requirements (MMR) for planning, coordinating and managing EW activities focused on mission execution. Future increments, including support to EW, integration for threat assessment, planning and coordination of force employment, operational reporting, Navigation Warfare and Spectrum Management related tools will follow as well as cueing to/from other functional services. An agile acquisition approach to C2 of EW should ensure the timely fulfilment of the highest prioritised requirements. This approach should also allow for added functionality as NATO EMO evolves.

An information exchange requirements working group is currently reviewing and updating existing NATO EW messages to ensure their

[9] *AJP 3.6 "ALLIED JOINT DOCTRINE FOR ELECTRONIC WARFARE".*
[10] *Ibid. 9.*

relevance and actuality. As a result, the NATO Common Electronic Order of Battle (C-EOB) exchange format will be introduced.

The C2 of EW supports NATO's exploitation of the EME from stabilisation or humanitarian operations through to major combat operations, ranging in scope from a single radio-controlled improvised-explosive device incident to operations against sophisticated Integrated Air Defence Systems (IADS). C2 of EW is by design intended to enhance the knowledge of the EME and inform Commander's decisions with the ultimate goal being to achieve EMS superiority.

NATO Emitter Database Next Generation

The NATO Emitter Database (NEDB) was established as a NATO database and information sharing tool on electromagnetic systems over 25 years ago. Recent operational requirements and technological developments triggered a technology uplift of the NEDB into the NATO Emitter Database Next Generation (NEDB-NG).

The NATO Emitter Database (NEDB) was established as a NATO database and information sharing tool on electromagnetic systems over 25 years ago. It is NATO's primary platform for EW mutual support and exchange of the best emitter data available in both peacetime and periods of crisis. Therefore, it is one of the most important sources of information to enable C2 of EW. Since its inception, the NEDB has been continuously expanded to facilitate the description of new electromagnetic systems and associated platforms.

Recent operational requirements and technological developments triggered a technology uplift of the NEDB into the NATO Emitter Database Next Generation (NEDB-NG). The existing database does not effectively address NATO's emitter data management processes, network security policies and lacks automation and integration with other information capabilities. There is also a requirement for a more complex data model that can adequately describe the complex modern emitters which continue to proliferate within the electromagnetic environment.

The NEDB-NG will be delivered during the first increment of C2 of EW. It was developed as a web-based capability, with advanced data storage and near real-time data-sharing capabilities, which can be deployed in a federated infrastructure of a system of systems. All existing NEDB data will be migrated into NEDB-NG which will be available and run on the NATO Secret Wide Area Network. It will also be accessible through Battlefield Information Collection and Exploitation Systems (BICES) networks to all NATO nations. Each NATO nation may also have national instances of NEDB-NG running on their own National networks.

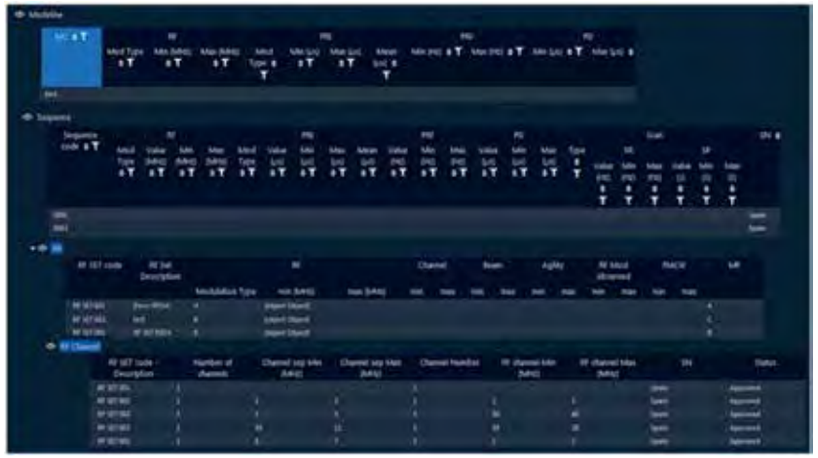


Figure 3: NEDB-NG Mock-up used to support the design of the Database Reader View. The image shows the filters available at the mode line level.

The NATO Recognised Electromagnetic Picture (REMP) aims to visualise EM activity in time and space (3D tracking) in a manner that is relevant to enhance situational awareness and the effective conduct of Allied EMO.

NATO Recognised Electromagnetic Picture

The NATO Recognised Electromagnetic Picture (REMP) aims to visualise EM activity in time and space (3D tracking) in a manner that is relevant to enhance situational awareness and the effective conduct of Allied EMO. NATO REMP seeks to compile all EOI for own, adversarial and neutral entities within the Joint Operations Area (JOA). The NATO REMP will utilise NATO Core Geographical Information Services (NATO Core GIS) to visualise geographically referenced EM information for dissemination and storage. As such it will provide a seamless sharing of the REMP into the NATO Common Operational Picture (NCOP), increasing the awareness of EMO across the Joint Force.

The NATO REMP will be a core function of NATO's future C2 of EW and will support the full range of features required for NATO EMO including planning, directing, monitoring and assessment of the EMO. Key to the support of planning and assessment of Allied EMO is the monitoring of near real-time universal EM activities to direct own forces' EM actions and capabilities in a congested and contested Electromagnetic Spectrum (EMS). Additionally, the NATO REMP will visualise the Electronic Order of Battle (EOB), showcasing the full EMS capability of platforms or force elements within the required area. The planning function of the NATO REMP will support the identified need for an agile approach to EMO. Modern military operations require constant refinement of own EMO. Own EMO will be planned and assessed

through digitalised modelling and propagation of EM sequences for each operational phase and account for the relevant terrain. The NATO REMP will facilitate reduced Electromagnetic Interference (EMI) within the Joint Forces through a shared understanding between the EW and Spectrum Management communities.

The NATO REMP enables the visualisation of the EME by bringing together NATO's EMO capabilities in a unified and coherent way. It will support NATO's wider EMO community of interest well beyond EW.

Conclusion

With C2 of EW functional services in place, the recovery scenario could continue up to the point of a successful extraction of the crew and recovery of critical materials like crypto and other technological advances which keep allied forces ahead of the adversary. The EWCC would provide an overview of threats and other activities in the EME for the overall mission planning and execution. Based on available data, EW sensors and self-protection equipment on the extracting assets could be updated to meet the current threats. This however also demands the near real-time collaboration with national EW reprogramming units. The joint restricted frequency list would be updated and prioritised to optimise the undisrupted Command, Control and Coordination of own forces. All completed with increased accuracy of information, speed and agility in the employment and integration of EMO.

The NATO EW community has developed a very mature set of criteria for C2 of EW based on an in-depth study of command and control in general and the C2 of EW specifically. The EW study includes a full review of NATO's EW information flow, formatting and usability. With these functional services, NATO will have a clear picture of the EME in the operational area, enabling effective EMO as another layer in the achievement of mission objectives and enabling the protection of own forces.

The future EME will require an advanced understanding of EME enabling exploitation, offensive and defensive EMO. NATO will be prepared by ensuring that the EMO community and EW Operators have the right tools to achieve EME superiority.

The future EME will require an advanced understanding of EME enabling exploitation, offensive and defensive EMO. NATO will be prepared by ensuring that the EMO community and EW Operators have the right tools to achieve EME superiority.

"EW has been a sleeping dragon, hidden away and forgotten for a generation. Now the awakened dragon needs to be controlled!"

MILESTONES IN THE COOPERATION BETWEEN THE USSR AND THE PEOPLE'S REPUBLIC OF CHINA DURING THE 1949-1991 PERIOD – A HISTORICAL PERSPECTIVE –

Colonel (r.) Eugen LUNGU, PhD
Faculty of Communication and International Relations, "Titu Maiorescu" University, Bucharest

Overall, the relations between the USSR and the People's Republic of China, the most powerful states of the communist world, were not at all satisfactory to the communist leaders in Moscow and Beijing. Historical documents reveal that the failed relations were about to degenerate into an armed conflict at some point. The paper is intended to highlight the key aspects in the history of the relations between the USSR and the People's Republic of China during the 1949-1991 period, and to bring to the fore the causes of the poor cooperation, a failure that further aggravated the negative image of the communist states during the Cold War period.

The significant feature of the present research is the fact that it was conducted considering the history of international relations, the main research method being the analysis of relevant documents relating to the Sino-Soviet relations between 1949 and 1991.

Keywords: USSR, People's Republic of China, Sino-Soviet cooperation, state actors, multipolar world.

English version by **Diana Cristiana LUPU**.

Introduction

The US global power, thoroughly demonstrated at the end of the Cold War, started to be denied by some state actors in the international arena, especially under the circumstances generated by the fact that the norms promoted by Washington in the international environment got to collide with the interests of certain regional powers. The successive events occurred in the nearly thirty years since the fall of the Berlin Wall have demonstrated that the Russian Federation and China are the states that opposed to many of the global policies initiated by Washington, and disputed, in different situations, the US military interventions having a humanitarian goal, promoting, not only within international organisations but also through foreign policy actions, the idea that a multipolar world should be acknowledged. Such an option, supported by Russia and China, is doctrinally based on the idea advocated by certain theorists of international relations that peace is best maintained by a relatively equal distribution of power, a condition for no state to be able to win a confrontation with a concurrent state[1].

The rapprochement between the two states in recent years, increasingly evident to anyone studying contemporary international relations, is one of the reasons for a more in-depth research into the relations of cooperation between Moscow and Beijing in the historical period previous to the one the two countries are currently going through, namely that characterised by the establishment of the People's Republic of China and the dissolution of the USSR.

The triumph of liberal order, backed by a number of Western theorists after the dissolution of the USSR, or *"The End of History"*, as Francis Fukuyama coins the victory of social systems based on the principles of liberal democracy in relation to Marxist-Leninist societies,

The triumph of liberal order, backed by a number of Western theorists after the dissolution of the USSR, or "The End of History", as Francis Fukuyama coins the victory of social systems based on the principles of liberal democracy in relation to Marxist-Leninist societies, generated a wave of frustration in geopolitical and geostrategic terms, starting in the late period of the last century, in both Moscow and Beijing, frustration amplified by the way the US has established itself as an absolute leader in global politics.

[1] Joshua S. Goldstein and Jon C. Pevehause, *Relații internaționale*, Editura Polirom, Iași, 2008, p. 126.

generated a wave of frustration in geopolitical and geostrategic terms, starting in the late period of the last century, in both Moscow and Beijing, frustration amplified by the way the US has established itself as an absolute leader in global politics. The will of the Russian Federation and China, as permanent members of the UN Security Council, to veto the policy globally promoted by the United States as the leader of the international relations system was the main reason for the rapprochement between the two states, out of the need to restore the global balance of power.

The People's Republic of China will celebrate, on 1 October this year, seven decades of existence, in an increasingly changing global context, whereby the major state actors of the current world generate, through their actions in world politics, a new tendency to regroup states, to preserve their own interests, thus influencing the regional balance of power as well as the entire system of international relations.

The People's Republic of China will celebrate, on 1 October this year, seven decades of existence, in an increasingly changing global context, whereby the major state actors of the current world generate, through their actions in world politics, a new tendency to regroup states, to preserve their own interests, thus influencing the regional balance of power as well as the entire system of international relations. The strategic partnership between the Russian Federation and China, signed in 1996, as well as the five-year-long treaty of friendship and good neighbourly relations between Moscow and Beijing are the major diplomatic milestones that laid the foundations for a new and solid cooperation in the political, economic and military domains between the two states, without any negative influence from the Soviet period. This strategic rapprochement between Russia and China, two revisionist powers, as they are currently referred to in Washington's official documents, and the geopolitical games generated by the Russian-Chinese alliance on all continents tend to erode the foundations of the liberal order, according to certain experts in international relations.

Therefore, the major changes expected in the global policy during the next decades, having the USA, the Russian Federation and the People's Republic of China as main actors, which may reconfigure the global balance of power, require for experts in international relations to thoroughly study the historical relations between Russia and China. The studies will certainly result in better understanding the current attitude of Moscow to cooperate with Beijing. Moreover, it is possible for the particular studies to reveal the fact that the historical cooperation between the two states is less important than their national interests.

In this study we intend to make a brief historical incursion to reflect the most important aspects of the Sino-Soviet relations during the 1949-1991 period, assessing, in a general manner, what the scope of the cooperation between the two states was at the end of the Soviet era. We know, and the diplomatic history demonstrates it, that, more often than not, the foreign policy strategies of the states cannot be detached from certain clichés of the past, and certain shortcomings in the past tend to overshadow even the best intentions of the new generations of diplomats. However, there are exceptions to these *"rules"*, as the political realism of some heads of state proves more important than the historical tradition, when national interests come first.

Given the current strategic relationship between the Russian Federation and the People's Republic of China as well as the fact that these two major state actors often challenge the US position as the leader of current world politics, it is important for international relations specialists and security researchers to have knowledge of the level of cooperation between the two states during the Soviet period and of the extent to which the Sino-Soviet relations between 1949 and 1991 constituted a solid basis for developing cooperation in the new geopolitical context, following the dissolution of the USSR.

Starting from the fact that the current relationship between Moscow and Beijing is a topic of major concern to many international relations and security studies, we consider that a brief incursion into the history of cooperation between the two states – especially in the political and military fields – can be beneficial from the perspective of a better understanding of the present. Thus, we can have a general picture of the Sino-Soviet cooperation relations during a period of over four decades, a picture that was less known to the older generations of people interested in studying the history of international relations in the former communist states, up to 1989, because of existing strict censorship.

Given the current strategic relationship between the Russian Federation and the People's Republic of China as well as the fact that these two major state actors often challenge the US position as the leader of current world politics, it is important for international relations specialists and security researchers to have knowledge of the level of cooperation between the two states during the Soviet period and of the extent to which the Sino-Soviet relations between 1949 and 1991 constituted a solid basis for developing cooperation in the new geopolitical context, following the dissolution of the USSR. Explaining the relations of cooperation between Russia and China over more than four decades, an important historical period from the standpoint of identifying the foreign policy practices and mechanisms promoted by each of these two countries, is also

an essential condition for understanding the way in which the historical factor, the traditional diplomatic relations between these two countries, may or may not influence the foreign and security policies promoted by the two states in the 21st century.

Milestones in the Sino-Soviet Relations in the Era of Stalin and Khrushchev

The Cold War period was one of confrontation between the East and the West at all levels, as it is presented in the vast literature, but at the same time it was a fierce battle between capitalism and communism all over the world, where the interests of the states belonging to the two political-social systems intersected. As the Canadian historian David R. Marples points out, referring to the Cold War apogee, *"the world had been divided into two hostile camps the Soviet propaganda had defined as capitalist and socialist"*[2]. It is known that the USSR, the state that represented, alongside the USA, one of the two major pillars of global order after 1945, was the country that led and coordinated the group of European Communist states on the Cold War front. Even if there were no direct armed clashes between the USSR-led communist camp and the US-led capitalist one, the history of that period, lasting for over four decades,registered armed conflicts between various Asian and African states, belligerent camps being supported by either the USA and its allies or by the USSR and its allies.

It is known that the USSR, the state that represented, alongside the USA, one of the two major pillars of global order after 1945, was the country that led and coordinated the group of European Communist states on the Cold War front.

As Michael Lynch points out, in an interesting paper on China after 1949, referring to the future of relations between the Soviets and the Chinese, *"all signs led to the idea that the People's Republic of China and the USSR will develop a very close partnership"*[3] and, as Mao Zedong states, *"Communist China, with regard to foreign policy, will rely one side only, namely on the Soviet Union"*[4]. Even though Mao showed respect in relation to the Soviet state and its leader, fact revealed by many historical documents of that time, the personal relationship between Mao and Stalin was, in most cases, a dysfunctional one.

[2] David R. Marples, *Rusia în secolul XX*, Editura Meteor Press, București, 2014, p. 286.
[3] Michael Lynch, *Republica Populară Chineză după 1949*, Editura All, București, 2004, p. 145.
[4] *Ibidem.*

Why did Communist China, right from the beginning of the establishment of the popular regime, opt for rapprochement with the USSR? A conclusive answer in this regard is given by Rana Mitter, a well-known British historian of Indian origin, specialised in China's history: *"China's turning towards the USSR after 1949 had an ideological nature, and it was a combination of political inclination and lack of other variants"*[5]. However, like other ideologies, international Marxism would split into several ideological trends, resulting in powerful disputes within the global communist movement, each party claiming to reach the ultimate truth as far as the construction of socialist society in its own country was concerned.

Why did Communist China, right from the beginning of the establishment of the popular regime, opt for rapprochement with the USSR? A conclusive answer in this regard is given by Rana Mitter, a well-known British historian of Indian origin, specialised in China's history: "China's turning towards the USSR after 1949 had an ideological nature, and it was a combination of political inclination and lack of other variants".

Given the different ways in which each communist party materialised Marxism-Leninism in own country, it can be assessed that the relation between the USSR and the People's Republic of China was far from being a model for the states in the socialist camp during the Cold War. Thus, the main characteristic of that relation was the existence of long periods of tension between Moscow and Beijing, caused by the significant differences in terms of ideology, especially following Stalin's death in 1953, as well as by territorial claims. As highlighted by the famous French author, Hélène Carrère d'Encausse, specialised in the history of Russia, the ideological authority of the USSR, the first communist state in the world, was contested by China only[6].

The history of Sino-Soviet relations after the end of the Second World War registered a series of important events – the visit of Chinese President Mao Zedong to Moscow, in February 1950 (the Cold War history records that Mao Zedong left China only twice, each time to visit the USSR) and the signing of the Treaty of Friendship Cooperation and Mutual Assistance; the visit of Russian President Nikita Khrushchev to China in December 1954; the visit of President Mikhail Gorbachev to China in May 1989. However, all the mentioned aspects could not change the overall impression in the Cold War period that the relations between the two communist states were tense. Moreover, the term

[5] Rana Mitter, *Calea amară a Chinei. Confruntarea cu lumea modernă*, Editura BIC ALL, Bucureşti, 2005, p. 147.
[6] Hélène Carrère d'Encausse, *URSS a murit, trăiască Rusia*, Editura Artemis, Bucureşti, 2010, p. 107.

"Sino-Soviet split" is often mentioned in the literature, referring to the nature of the relations between the USSR and the People's Republic of China during the Cold War period, relations disrupted by the ideological differences in interpreting Marxist ideology, expressed starting in the mid '50s up to the dissolution of the USSR. The statement made by Henry Kissinger regarding the Sino-Soviet split on ideological grounds is relevant in this context: *"It was ideology that put China and Russia either on or off"*[7].

Having a thorough look at the history of Sino-Soviet relations in the last century, it can be noticed that Khrushchev's denunciation of the policies promoted by Stalin against his own people, at the 20th Congress of the Communist Party of the USSR, in 1956, did not have a positive echo in the People's Republic of China. Many authors specialised in the Cold War history express the opinion that Khrushchev's rupture with Stalin's policy was a direct affront to China because the Chinese had adhered to the Stalinist doctrine as a recognition of the role played by the Soviet ruler during the Second World War[8]. Moreover, considering the ideological affinities between the Chinese Communist Party leadership and Stalin's policies, Khrushchev was perceived as a president incapable of capitalising on the positive heritage of the foreign policy promoted by Stalin, *"a Trotskyist traitor"*[9], *inconsistent in developing equal relations with the USA: "Khrushchev's first major change in politics in the post-Stalinist era, the 1956 secret speech that was immediately disclosed, which condemned Stalin's terror, led to a major change in Chinese politics. Mao was angry at what he considered betrayal, and the Hungarian revolution in the same year convinced him that it was time to try a political liberalization"*[10], according to Rana Mitter.

Many authors specialised in the Cold War history express the opinion that Khrushchev's rupture with Stalin's policy was a direct affront to China because the Chinese had adhered to the Stalinist doctrine as a recognition of the role played by the Soviet ruler during the Second World War.

As far as China in the '50s was concerned, it should be noted that not only the leaders of the state but also the largest part of the population still felt the wounds caused by the *"nineteenth-century and early-twentieth-century extraterritoriality agreements by which*

[7] Henry Kissinger, *Despre China*, 2nd Edition, Editura Comunicare.ro, Bucureşti, 2018, p. 167.
[8] Michael Lynch, *op. cit.*, p. 269.
[9] Rana Mitter, *op. cit.*, p. 147.
[10] *Ibidem*, p. 144.

Western nations took control over parts of Chinese cities"[11]. They were regarded as equally humiliating to China as were the territorial losses of the 19th-century dynastic Qing Empire (Nepal and Burma in favour of Great Britain, Indochina in favour of France, Taiwan and Sahalin in favour of Japan, Amuria, Usury and Mongolia in favour of Russia[12]). All the mentioned unfavourable events, concerning territorial issues for the history of China in the 19th and 20th centuries, come to justify the irredentist spirit of Mao Zedong, the leader who also managed to convey to the Chinese people his inner suffering about the fact that China had been humiliated with the loss of important regions in favour of foreign, European and Asian powers. The emergence of maps with Great China in the 1950s, including the territories lost in the 19th and 20th centuries, even in Chinese middle schools, support the idea of irredentist tendencies officially promoted by China and accepted up to the highest levels of the state government.

Three years after Joseph Vissarionovich Stalin died, Khrushchev's criticism directed against the cult of personality and the abuses committed by the Stalinist leadership over the Soviet people opened the way for doctrinal dissensions between China and the USSR in terms of interpreting Marxist-Leninist teachings. The fundamental ideological differences were to be further amplified by the Chinese side in the years to come, in the context of a Soviet interventionist geopolitics in which Moscow, contrary to the principles established at the level of the socialist state community, intervened militarily in the domestic affairs of other states (Hungary – 1956, Czechoslovakia – 1968, Afghanistan – 1980-1989). Moreover, the disagreements between the two states got manifest in 1959, the year when the Chinese revoked an agreement signed with the USSR four years before, by which the Soviets had committed themselves to supporting China in the production of the nuclear weapon. Against the background of the disputes between the two states, China expelled the Soviet advisers and technicians who had been sent by the Soviet state to provide technical assistance to the Chinese state in the field of nuclear

Three years after Joseph Vissarionovich Stalin died, Khrushchev's criticism directed against the cult of personality and the abuses committed by the Stalinist leadership over the Soviet people opened the way for doctrinal dissensions between China and the USSR in terms of interpreting Marxist-Leninist teachings.

[11] Robert Kaplan, *Răzbunarea geografiei. Ce ne spune harta despre conflictele viitoare şi lupta împotriva destinului*, Editura Litera, Bucureşti, 2014, p. 267.
[12] *Ibidem*, p. 266.

technology. In the context of the increasingly troubled relations between the USSR and China, Khrushchev offered support to India in the conflicts with China, in 1959 and 1962, and the states in the socialist camp, through their foreign policies, considering the power available to each of the two major communist states, had to rally to either the USSR or China.

Cooperation between Moscow and Beijing in the Era of Brezhnev and Gorbachev

It can be said that in the "Brezhnev Era" the ideological tensions between China and the USSR increased because of the fact that Moscow used the military force outside the country, by virtue of the "Brezhnev Doctrine" (the Limited Sovereignty Doctrine), highlighting that the Soviet regime was imperial in all respects.

In the '70s, when the leader of the USSR was Leonid Brezhnev, the relations between the USSR and China remained tense, without any change in substance compared to the Khrushchev time. To the major ideological differences there were added the dissensions regarding the ownership of the territories situated at the border between the two states. Thus, although in foreign policy Moscow did not cease to promote the most generous principles of peaceful coexistence between states and nations, between 1964 and 1982, when Leonid Brezhnev ruled the Soviet Union, there were some *"frontier"* military confrontations between the USSR and China. According to David R. Marples, in the Brezhnev era, China was no longer a rival power to the Kremlin regime, but it became the main enemy of the USSR[13]. The sharp Sino-Soviet rivalry, which was blatantly manifested during more than two decades when Brezhnev ruled the Soviet Union, generated, according to many international relations historians, measures in the field of military security taken by both sides as well as by other state actors, which contributed to the slow change in the global balance of power. There are studies stating that the Sino-Soviet rivalry during the Cold War period somehow changed the geopolitics of the time from a bipolar confrontation, with the USSR and the USA as main actors, to a tripolar one, the People's Republic of China being added to them. It can be said, therefore, that in the *"Brezhnev Era"* the ideological tensions between China and the USSR increased because of the fact that Moscow used the military force outside the country, by virtue of the *"Brezhnev Doctrine"* (the Limited Sovereignty Doctrine), highlighting that the Soviet regime was imperial in all respects.

[13] David R. Marples, *op. cit.*, p. 329.

The failure of the relations with China led President Brezhnev to seek allies in Asia to generate a favourable balance of power, given the common border between the two states. The USSR attempts to develop partnerships with Asian states in order to build strategic barriers on the direction to China were unsuccessful. Vietnam was the only exception, a country with which China had a conflict in 1979. Otherwise, the Soviet approaches did not generate favourable results for Moscow in Asia. Mention should be made, however, that the USA capitalised on the dissensions within the communist camp, achieving, through President Richard Nixon and Secretary of State Henry Kissinger, a real diplomatic coup during the Cold War period, namely the establishment of diplomatic relations between the USA and China in 1972. David Marples words are edifying in this regard: *"In 1972, following the initiative of US President, Richard Nixon, and Secretary of State, Henry Kissinger, the USA and China established diplomatic relations, a great step backwards for the USSR, which was unexpectedly faced with the possibility, so feared by Stalin, of being surrounded by hostile states"*[14].

The USA capitalised on the dissensions within the communist camp, achieving, through President Richard Nixon and Secretary of State Henry Kissinger, a real diplomatic coup during the Cold War period, namely the establishment of diplomatic relations between the USA and China in 1972.

The death, in 1976, of Chinese President Mao Zedong, the one with whom Moscow had no cordial relations, failed to ease the tense relations between the two communist states because of the important ideological differences. The Chinese authorities continued the accusations of imperialism as a result of the interference of Soviet power in the internal affairs of other states and especially the military campaign in Afghanistan, launched in 1979. That war, which, since its debut, surprised the entire international community and the support the two Communist states provided for rival clients in Southeast Asia (China supported Cambodia while the USSR supported Vietnam) were important aspects that characterised the foreign policy profile of the two countries, which hindered the improvement of the relations between them.

It can be stated that, in the Brezhnev era[15], the relations between China and the USSR were troubled, and the inability of the Soviet

[14] *Ibidem*, p. 344.

[15] There are opinions expressed in the literature according to which Leonid Brezhnev was Sino-phobic, the reason why he, as Head of State, could not adopt effective measures to enhance the relations with the People's Republic of China.

diplomacy to enhance the collaboration with the Chinese party provided the West with a considerable advantage in relation to the communist camp, the Soviet Union losing its credibility as the true leader of communism worldwide. How the hostile relations between the two communist states contributed to the erosion of the communist world from within, and how the failed Sino-Soviet relationship contributed to hastening the end of the Cold War are two questions to which we do not intend to respond in this study. However, what we can state without fear of being wrong is that the relations between the USSR and China, the largest communist states of the Cold War world, did not represent a model to follow for the other communist states, spurring the anti-Communist movements in the West and in the world, which managed to capitalise on the political failures of communism for propaganda purposes.

It can be stated that, in the Brezhnev era, the relations between China and the USSR were troubled, and the inability of the Soviet diplomacy to enhance the collaboration with the Chinese party provided the West with a considerable advantage in relation to the communist camp, the Soviet Union losing its credibility as the true leader of communism worldwide.

The nuclear arms race, one of the essential features of the Cold War era, had the USSR and the USA as main actors. However, communist China, which later entered into the restricted group of nuclear states, did not neglect this state defence sector. The first country that achieved the nuclear weapon was, as it is known, the United States of America, in 1945, followed by the USSR only four years later, on 29 August 1949, when the communist regime in Moscow detonated the first nuclear bomb, an event that marked the cessation of the US atomic monopoly. Starting in the ’50s, China began to develop its military nuclear programme, being technologically supported, during the first years, by the USSR, in a spirit of solidarity with the Chinese membership of the great family of communist states in the world. However, once the ideological dissensions between China and the USSR emerged, in the summer of 1959, Nikita Khrushchev decided to suspend the Soviet support for the nuclear programme of China. Under such circumstances, China continued its nuclear research, without Soviet support, and it detonated the first Chinese nuclear bomb in the Sinkiang desert, in the northwest of the country, in October 1964.

Although China, with own forces, succeeded in completing the nuclear programme intended for the production of the first atomic bomb, the Kremlin used to affirm that the aid provided for Beijing in the first stage of the nuclear programme development was decisive.

It would be also confirmed by Leonid Ilyich Brezhnev, the General Secretary of the Central Committee of the Communist Party of the Soviet Union (CPSU), during a meeting with the Romanian delegation led by President Nicolae Ceauşescu, in March 1967, in Moscow: *“If we, the Soviets, had not helped them, the Chinese would have never produced the atomic bomb; it is not a secret, we can say it now”*[16]. Therefore, despite ideological dissensions, the relation between China and the USSR in the nuclear programme, although limited in scope and short in time, was beneficial for the Chinese, in terms of strengthening the country’s defence capability.

The death of Soviet President Leonid Brezhnev in 1982 as well as the major changes generated by China’s openness in terms of economic policy and foreign policy resulted in starting the rapprochement between the Soviet Union and China. Two-year consultations were established to normalise the relations, but the Chinese did not renounce invoking the obstacles to improving the relations between Beijing and Moscow in the past years: the presence of Russian soldiers in Afghanistan; the stationing of Russian soldiers near the border between the USSR and China as well as in Mongolia; the Soviet support for Vietnam to invade Cambodia.

A major change occurred when Mikhail Gorbachev came to power in 1985, when the Sino-Soviet relations started to improve in terms of economic exchanges, technological assistance, and modernisation of some projects built with Soviet assistance in the ’50s. Although Mikhail Gorbachev acknowledged the USSR political mistakes in relation to China, it should be noted that he inherited an extremely rigid foreign policy from his predecessors, and his attempts to restructuring and reforming it were barely accepted by the hard, traditionalist core of the Kremlin communist leadership. However, in an extremely important speech delivered in July 1986, in Vladivostok, Mikhail Gorbachev proved to be the first Russian President who demonstrated flexibility in the relations with China, launching several initiatives regarding the USSR policies in the Asia-Pacific region. Moreover, it was announced a new

A major change occurred when Mikhail Gorbachev came to power in 1985, when the Sino-Soviet relations started to improve in terms of economic exchanges, technological assistance, and modernisation of some projects built with Soviet assistance in the ’50s. Although Mikhail Gorbachev acknowledged the USSR political mistakes in relation to China, it should be noted that he inherited an extremely rigid foreign policy from his predecessors, and his attempts to restructuring and reforming it were barely accepted by the hard, traditionalist core of the Kremlin communist leadership.

[16] Stenogram of the high-level talks between the CPSU and the RCP, 17-18 March 1967, Moscow, in *România şi negocierea Tratatului de neproliferarea armelor nucleare*, coordinator Nicolae Ecobescu, Fundația Europeană Titulescu, Bucureşti, 2016, p. 231.

vision regarding the USSR further cooperation with Asian neighbours – China, Japan and South Korea.

Beijing welcomed Gorbachev's proposals on the joint development of a space programme, the agreement on railways in the border area, the development of a programme on hydroelectric power plants, and the announcement of the partial withdrawal of Russian troops from Afghanistan and Mongolia. Regarding the *"Vladivostok moment"* and its historical significance for the relations between the USSR and China, Hélène Carrère d'Encausse states that *"the Russian-Chinese reconciliation – after the tough dispute of the 1950s – started in 1986, when Mikhail Gorbachev proclaimed, in Vladivostok, the need for the two major socialist states to establish harmonious relations in order to create an area of peace and friendship"*[17].

Even though the outcomes of the foreign policy with China in the Gorbachev era were not very spectacular, it can be said that it was extremely important for Russia that Gorbachev outlined a positive vision of cooperation with not only Asian but also European neighbours, totally different from that of his predecessors.

Although the USSR did not formally re-establish the relationship with the People's Republic of China by the end of the 1980s, it can still be said that the relations between the two states have improved significantly in comparison with the previous decades. Even though the outcomes of the foreign policy with China in the Gorbachev era were not very spectacular, it can be said that it was extremely important for Russia that Gorbachev outlined a positive vision of cooperation with not only Asian but also European neighbours, totally different from that of his predecessors. The openness demonstrated by Gorbachev in relation to China was fundamental, because in the years following the collapse of the USSR, the Kremlin leaders could benefit from a new Russian-Chinese cooperation platform built by President Gorbachev, which was totally different from that inherited from Khrushchev or Brezhnev.

Conclusions

It can be seen from the information presented that, for more than the four decades we have referred to in this study, overlapping most of the Cold War history, the scope of cooperation between the USSR and the People's Republic of China was quite narrow. The vanity was high, in both Moscow and Beijing, and the ideological contradictions between the two major communist states were so strong that real

[17] Hélène Carrère d'Encausse, *op. cit.*, p. 20.

closeness was impossible and thaw did not occur even after the physical disappearance of Mao and Brezhnev.

The Soviet Union always wanted to impose itself in its relations with communist China as a bigger *"sister"* born in 1917 compared to the other popular regime created in 1949, thus trying to widen the sphere of influence within the socialist camp over the Asian continent too. However, all Moscow attempts in the post-Stalinist era were met with the firm opposition of Beijing, convinced that the Soviet Union deviated from the principles and ideals of Marxism-Leninism. The 1956 revolutionary movement in Hungary, where the stationing Soviet troops acted in force killing about 2,500 Hungarian citizens, as well as the those that followed – Czechoslovakia - 1968, Afghanistan - 1979 – fuelled and maintained the total distrust of Beijing in the Kremlin's interventionist policy, making the reconciliation between the two communist states impossible.

The Soviet Union always wanted to impose itself in its relations with communist China as a bigger "sister" born in 1917 compared to the other popular regime created in 1949, thus trying to widen the sphere of influence within the socialist camp over the Asian continent too. However, all Moscow attempts in the post-Stalinist era were met with the firm opposition of Beijing, convinced that the Soviet Union deviated from the principles and ideals of Marxism-Leninism.

This brief analysis of the Sino-Soviet relations, as part of the history of international relations, highlights a number of political, ideological and security issues. It reveals that the scope of cooperative relations between the USSR and the People's Republic of China used to be narrow. However, we currently find out, through the media, that the two states have a strategic partnership, materialised in achievements in diverse areas. Therefore, looking at how the relations between the two states have evolved in the almost thirty years that have passed since the fall of the Berlin Wall, the conclusions are totally different compared to the 1949-1991 period. Having extremely pragmatic leaders since 1991, the two states have managed to get rid of the entire residual stress of the Soviet-era history, where the key word was *"confrontation"*, and to look at the future from a perspective where what matters is just the national interests of both countries.

Considering that the presidents of the two states, Vladimir Putin and his Chinese counter part, Xi Jinping, have met for 28 times in the past six years, and the volume of trade between Russia and China exceeded, in 2018, the amount of 100 billion dollars, we can easily acknowledge the current level of political and economic cooperation between the two states[18]. Moreover, there is a high level of military cooperation

[18] Miodrag Soric, *China şi Rusia – doi parteneri inegali*, Focul Media Center, see https://www.dw.com/ro/china-%C8%99i-rusia-doi-parteneri-inegali/a-49061700, retrieved on 09.07.2019.

between the two countries within the Shanghai Cooperation Organisation, which triggers extra attention from Washington, given the major US interest in the Asia-Pacific region. The large-scale military manoeuvres in the fall of 2018 – *"Vostok 2018"*, which took place between 11-17 September 2018 in Siberia, the Russian Far East, and the Sea of Japan, with the participation of about 300,000 Russian soldiers and about 3,000 Chinese soldiers, 36,000 vehicles, 1,000 airplanes, helicopters and drones, and 80 ships – were a real show of force conveying a *"message"* not only to the entire Asia but also to Washington, against the background of the deterioration of China-USA economic relations on the grounds of commercial protectionism.

The cooperation relations between the Russians and the Chinese can be characterised using totally different terms. Thus, up to the dissolution of the USSR, ideological factors hindered the cooperation between Moscow and Beijing. After 1991, it was the political realism doctrine that made the two states develop an important strategic partnership in different domains.

Considering the two historical periods, 1949-1991 and 1991-2019, it can be concluded that the cooperation relations between the Russians and the Chinese can be characterised using totally different terms. Thus, up to the dissolution of the USSR, ideological factors hindered the cooperation between Moscow and Beijing. After 1991, it was the political realism doctrine that made the two states develop an important strategic partnership in different domains. However, there are experts in international relations who openly mention the *"marriage of convenience"* between Russia and China, as their divergent interests, rooted in the past, related to the Asian space geopolitics, will become evident in the years to follow. Therefore, the old disagreements, previous to the dissolution of the USSR, somehow *"silenced"* currently will reappear in a different form, once the first dissensions occur between the two states leaderships.

Without giving full credibility to theories such as the above-mentioned one, it remains an extremely trenchant question that has its origin in the essence of this study: *Will the pragmatic statesmen in Moscow and Beijing manage to be immune to any negative influence rooted in the history of Sino-Soviet relations?*

BIBLIOGRAPHY

1. Hélène Carrère d'Encausse, *URSS a murit, trăiască Rusia*, Editura Artemis, Bucureşti, 2010.
2. Joshua S. Goldstein and Jon C. Pevehause, *Relații internaționale*, Editura Polirom, Iaşi, 2008.
3. Robert Kaplan, *Răzbunarea geografiei. Ce ne spune harta despre conflictele viitoare şi lupta împotriva destinului*, Editura Litera, Bucureşti, 2014.
4. Henry Kissinger, *Despre China*, 2nd Edition, Editura Comunicare.ro, Bucureşti, 2018.
5. Michael Lynch, *Republica Populară Chineză după 1949*, Editura All, Bucureşti, 2004.
6. David R. Marples, *Rusia în secolul XX*, Editura Meteor Press, Bucureşti, 2014.
7. Rana Mitter, *Calea amară a Chinei. Confruntarea cu lumea modernă*, Editura BIC ALL, Bucureşti, 2005.

Președintele României

Dorind a răsplăti meritele

revistei

„Gândirea militară românească"

cu ocazia împlinirii a 140 de ani de existență, pentru rezultatele deosebite obținute în întemeierea teoretică a 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 politico-militare,

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. Cav. 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 Ser. 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