

ISSN 2537-1363
ISSN-L 2537-1363

JOURNAL OF THE ACADEMY OF NATIONAL SECURITY SCIENCES - Issue no. 2/2019

RASSN



JOURNAL OF THE ACADEMY OF THE NATIONAL SECURITY SCIENCES

Issue no. 2/ **2019**

MILITARY SCIENCES

INTELLIGENCE AND NATIONAL SECURITY

PUBLIC ORDER

SCIENTIFIC BOARD

Prof. **Remus PRICOPIE**, PhD – President

Prof.dipl.eng, **Pavel NEČAS**, PhD, MBA, dr.h.c., Faculty of Political Science and International Relations, University of Matej Bel, Slovakia;
Assoc. prof. **Jan RAJCHEL** – University of Natural Sciences and Humanities, Poland;
Prof. **Miroslav KELEMEN**, Tehnical University of Košice, Slovakia;

Prof. **George MAIOR**, PhD
Prof. **Vasile DÎNCU**, PhD
Prof. **Gabriel-Florin MOISESCU**, PhD
Prof. **Adrian CURAJ**, PhD
Prof. **Gheorghe TOMA**, PhD
Prof. **Teodor FRUNZETI**, PhD
Prof. **Ion MITULETU**, PhD
Prof. **Cristian POPESCU**, PhD
Prof. **Gheorghe BOARU**, PhD
Prof. **Gheorghe BĂRBULESCU**, PhD
Prof. **Sorin CÎMPEANU**, PhD
Prof. **Viorel BUȚA**, PhD
Prof. **George ȚICAL**, PhD
Prof. **Adrian IACOB**, PhD
Prof. **Costel DUMITRESCU**, PhD
Prof. **Țuțu PIȘLEAG**, PhD
Assoc. prof. **Diana Elena ȚUȚUIANU**, PhD
Associ. prof. **Florin NEACȘA**, PhD
Petru ȚĂGOREAN, PhD

Editorial board

Publisher-in-chief - Prof. **Gheorghe BOARU**, PhD
Deputy Publisher-in-chief - Prof. **George-Marius ȚICAL**, PhD

Members

Prof. **Ion Mitulețu**, PhD
Prof. **Țuțu Pișleag**, PhD
Assoc. prof. **Diana-Elena Țuțuianu**, PhD
Nelușa Solbă

Secretary of editorial board – Assoc. prof. **Florin Neacșa**, PhD

*Journal of
The Academy of
National Security
Sciences*

Published by The Academy of National Security Sciences

*Nr. 2 (07)
Anul IV, 2019*



Journal indexed in international databases
(SRN, ResearchBib, Scipio)

ISSN 2537-1363
ISSN-L 2537-1363




CONTENTS

EDITORIAL	5
<i>Editorial Board</i>	
THE HISTORY OF INTERNATIONAL SECURITY – SOURCE OF SECURITY ASSUMPTIONS	9
<i>General (ret.) Professor Teodor FRUNZETI, PhD</i>	
<i>Colonel (ret.) Professor eng. Eugen SITEANU, PhD</i>	
INFORMATION WARFARE - AN OBJECTIVE OF NATIONAL SECURITY	22
<i>Colonel (ret.) Professor, Gheorghe BOARU, PhD</i>	
HYBRID WARFARE AND THE MARITIME COMPONENT. TOGETHER OR AS SEPARATE ENTITIES?	37
<i>Brigadier General (ret.) Professor Viorel BUȚA, PhD</i>	
<i>Lieutenant (Navy) Andrei PAVĂL, PhD student</i>	
APPROACHING MILITARY ART FROM A HERMENEUTICAL PERSPECTIVE.....	47
<i>Colonel (r.) Professor Ion MITULEȚU, PhD</i>	
IS IT TIME TO CHANGE THE MDMP WITHIN THE ROMANIAN ARMED FORCES?.....	63
<i>Brigadier General (ret.) Professor Viorel BUȚA, PhD</i>	
<i>Lieutenant Colonel Irinel APOSTOLESCU, PhD student</i>	



TANKS AND THEIR TACTICS – WHERE TO? 100 YEARS OF HISTORY	76
<i>Brigadier General (ret.) Professor Gheorghe TOMA, PhD</i>	
MAINTENANCE OF PUBLIC ORDER – BETWEEN SCIENCE AND ART.....	82
<i>Professor Țuțu Pișleag, PhD</i>	
ARTIFICIAL INTELLIGENCE AND ITS IMPACT ON SECURITY NATURAL DISASTERS, A GROWING HAZARD FOR WORLDWIDE STATES.....	99
<i>Colonel Associate Professor Engineer Florin NEACȘA, PhD</i>	
ARTIFICIAL INTELLIGENCE AND ITS IMPACT ON SECURITY.....	112
<i>Colonel Ion-Marius NICOLAE, PhD</i>	
PARTICULARITIES OF THE ROMANIAN MIGRATION IN THE POST COLD WAR PERIOD	133
<i>PhD student Alina ARDELEANU</i>	



EDITORIAL

**ARE THERE THREATS TO ROMANIA'S NATIONAL SECURITY?
WHAT ABOUT EUROPE'S SECURITY?**

In a permanently changing world, the European Union Security Agenda needs to be updated in such a manner so as to answer in the same parameters with the development of society. Awareness has been raised therefore on the fact that the role played by the EU in this field has to grow. The approach employed by the EU, regardless of its endeavors, is based on 's rights and on creating a common safe space. In order to try to diminish the effects of insecurity, we need to resort to the global role of the EU and the large range of instruments it has, understanding the common causes of certain dysfunctionalities. The profound character of causes and effects needs adopting a different approach.

The emergence of conflicts, sometimes armed ones, determine us to be much more careful to the game of international actors, especially when the wish for independence of some minorities leads to the escalation of the conflict up to the point of using armed force. Here, we need to focus mainly on the conflict at the borders of Turkey and the armed incidents where there are victims among the civilian population and there are other forces of global level in the area.

Nowadays, conflicts may start at peacetime and underneath its appearance, without a declaration of war, the aim being to seek for exploiting the enemy's political, economic, military vulnerabilities. The complexity of the political-military situation is very high and, we may even say that it is unpredictable. State actors may belong to the European, American or Asian space.

The actions taken are highly likely to be hybrid including, simultaneous or on stages, the conduct of information, economic, diplomatic and / or classical actions. It is possible to use first "nonmilitary means" and afterwards



to engage military force in order to intimidate and exercise pressure. The entities involved in hybrid threats may be state or non-state actors.

The defense solutions are quite numerous, but we consider that it is absolutely mandatory to apply early identification of the attack, activation of societal resilience factors and increasing them so as the state may be able to function in crisis circumstances too.

The use of, in case of hybrid warfare, of both conventional and non-conventional means, of both military and nonmilitary procedures, in a coordinated manner or separately, make defense planning a very complicated and difficult process.

European security and insecurity are also depending on certain social phenomena. The impact of global poverty and conflicts in the entire world are going beyond national borders. Europe should remain a refuge for those who are fleeing from persecution as well as an attractive destination for the talent and entrepreneurship of students, researchers, and workers generally speaking. Europe's reaction for these situations was immediate, but insufficient. A punctual relation is not sufficient, which lead to applying emergency measures, revealing a collective European policy in this field seriously lacking in certain regards.

Respecting international commitments and European values in the circumstances of securing the borders and at the same time creating the optimal conditions for economic welfare and societal cohesion in Europe represent a very difficult balancing exercise which necessitates coordinated actions at European level.

The common values which are the grounds of all European democratic and social models are the fundament of European freedom, security and prosperity.

Combatting radicalization, stimulating cybersecurity and reducing terrorism financing, as well as improving information exchange are all directions of action specified in the European Security Agenda that ends this year. This issue at European level is under close scrutiny nowadays and the future agenda is envisaged to have only four priorities, such as: protecting citizens and freedoms; developing a strong and competitive economic basis; building a Europe which is neuter from the climate point of view, green, correct and social; promoting the European interests and values on the global scene.



The European purpose is to continue the actions taken, together with the partners in each side of the world, in order to ensure durable policies that might have direct and real impact upon European security.

A priority which has already been established is protecting citizens and their freedoms. The European system of protecting human rights was set by the European Council, having as aim that *"each member of the European Council should embrace the principles of the rule of law state and the principle according to which each person under its jurisdiction enjoys the fundamental rights and freedoms of people"*.

The rule of law is a key hallmark for the fact that European or national values are protected; this principle needs to be fully respected by all member states and the EU. An integrated management of the borders is an absolute prior condition for guaranteeing security.

The European Union has actively supported national efforts of improving the management of migration flows, of managing border issues and security at the same time ensuring the necessary finances. Thus, the European political asylum is an issue that European Commission and European Council are constantly trying to answer to by the new policies adopted.

The correct functioning of Schengen Convention is a permanent European direction of action. The Schengen Area, one of the valuable accomplishments of European Union, is an area where there is free movement, where there is no more border control, a rule that also has many exceptions. Being part of Schengen Area implies a cooperation of all police forces in the member states, in order to combat organized crime or terrorism, especially through information exchange, in the same manner as in Schengen Information System (SIS).

Countering terrorism is a major priority for not only the EU and member states, but also for its international partners. Here is the main focus of nowadays fight through consolidating cooperation and information exchange, all these being achieved through the development of common instruments. Terrorism is a threat to European security, democratic values, as well as the freedoms and rights of European citizens.

A maximal priority is also that of transborder criminality, that has acquired an increasingly clearer shape at European level, from common criminality to that pertaining to organized crime. One of the issues that are still very problematic is drug trafficking with substances brought from



South America or the heroin and cannabis brought from the Gold Crescent (Afghanistan, Pakistan).

People trafficking, in order to exploit their work, has increased to the detriment of sexual exploitation people trafficking. Mixed groups, made up of local policemen and those belonging to the countries most likely to be subject to these crimes, may be an efficient solution for solving this issue.

Another goal is to increase EU's resilience against *natural disasters and especially those manmade*. Active solidarity and accumulation of resources are essential in this regard.

Another very important priority is protection against cyber actions. In order to efficiently put in practice cyber defense, there is a need for a set of basic measures as well as a clear and coherent common policy.

The current talks at the level of European Commission are focused on climate issues and on creating a green Europe. Thus, the European Commission has proposed a strategy until 2050 referring to the impact of the climate. The desire is to reach a certain neuter climate found in realistic technological solutions with an impact upon weather. This strategy relies on elements such as increasing the citizens' level of responsibility and prioritizing actions in key domains such as industrial policy or research.

Brexit also creates another paradigm that has not been disclosed yet. No matter how odd this may seem, this step which is still obscure and in large measure populist taken by individual political circles in Great Britain is able to significantly change the region and open up new opportunities, for many countries including Russia and Turkey. We notice that the new priorities of the future strategy are not outlined yet, being permanently analyzed so as to result in the most important ones, depending on the existing circumstances.

The thoughts expressed in this brief presentation are detailed in the scientific work of the authors who wrote the articles in this review in which they tried to exchange information or launch challenges that might lead to a continuous scientific dialogue and, why not, to certain conclusions to answer the question: "which are really the biggest threats to Romania's national security and even Europe's security? ".

Editorial Board



THE HISTORY OF INTERNATIONAL SECURITY – SOURCE OF SECURITY ASSUMPTIONS

General (ret.) Professor Teodor FRUNZETI, PhD

Tenured member of the Academy of National Security Sciences,
Tenured member of the Academy of Romanian Scientists,
E-mail: tfrunzeti@gmail.com

Colonel (ret.) Professor eng. Eugen SITEANU, PhD

Corresponding member of the Academy of Romanian Scientists,
Tenured member of the Romanian Committee of the History and
Philosophy of Science and Technology (CRIFST) of Romanian Academy,
E-mail: esiteanu@yahoo.com

Abstract: *The security assumption is the statement / assertion regarding the relation of causality that might be verified empirically. The assumption can be based on historic security knowledge or on certain events observed by the researcher, so the assumption is a reflection of certain connections between phenomena of security / insecurity observed by scientists. The security assumption may also be a supposition made by the researcher regarding connections between the phenomena of security / insecurity. The source of these assumptions may be the history of security, namely certain knowledge in history resulting in certain assumptions, or practical knowledge of security / insecurity.*

Keywords: *history of security, security assumptions, phenomena of security / insecurity, connections, source of assumptions.*

1. Introduction

An assumption or hypothesis in security science is a statement regarding a probable relation/link, usually the cause-effect type, which might be verified empirically. Any security hypothesis can be formulated based on historic evidence (obviously, prior) or on certain security events (facts) noticed by the researcher and it represents the probable link between the security or insecurity phenomena which had been already noticed.

The specific objectives of security research are given by certain working assumptions that need to be verified by researchers / scientists.



Thus, proposing a security hypothesis or assumption consists in the following: 1) the assertion or supposition of the scientist (researcher) regarding the connection /connections among certain security phenomena; 2) the supposition – which is based on certain knowledge or on prior research or on certain research results communicated regarding the respective connections (the connections may be based on probabilities or statistics); 3) a supposition regarding the kind of relationship in place (with one independent and one dependent variable); 4) the way leading to formulating a security theory that explains the respective phenomenon and allows for finding ways to solve the security issue.

Within the methodology of scientific research used in security science, we often find the method of document analysis, as data and information must be gathered in the research process, and the method of using research means for data processing (both analytical and synthetic processing).

Documents comprising scientific information in the field of security/insecurity are a main source in the security analysis. These documents may be inscriptions, texts (handwritten or printed), testimonials about security / insecurity events etc. There are a lot of historic documents, including those pertaining to military history or the history of security. This method of document analysis comprises several main stages: general analysis of information sources; study of information in the respective sources; critical assessment of information; a synthesis of the study performed and an interpretation of the researcher.

The analysis of documents that can be conducted by any researcher in order to re-construct the social-political-economic reality represents a research endeavor that may also resort to other research means such as observation, enquiry, case-study, logical method etc.

History provides us with extensive experience that cannot be acquired in any other way to achieve / produce / accomplish / acquire / obtain knowledge about various living styles in other times and places. As history also includes a huge amount of details / events that lack significance from the point of view of security, we only need those that are significant for security / insecurity and that can be found in two disciplines or sub-domains of history: military history and security history. The latter is a new subject matter, unlike military history. A philosophical question would be how to derive some useful security lessons from the huge amount of knowledge on



the past of mankind? Without this concern for using historic lessons for the current security of mankind, both our present and our future will be kept in the dark, without any prospect of seeing light soon. Thus, the history of security is actually the experience of mankind and ignoring it means that we will never be able to know who we are and how we have become what we are now. In turn, this will mean that we would lose our identity and we would forget feelings, values and ideals people have lived and fought for and some generations have even given up everything for. All these were turned into the starting point for forming peoples, nations, states, religions, etc. History discloses crimes against humanity and the heroism of past generations. History provides the perspective of moving present forces and a necessary basis for making a rational decision for future actions.

2. The dual character or dichotomy / symbiosis of security science

As risks, threats, and hazards come both from natural and socio-human phenomena (proving their dual character) various epistemologies are promoted in the science of security / insecurity:

- empirical epistemology (scientific statements containing observations that may be verified empirically);
- logical-formal epistemology (containing axiomatic system and a formal language);
- hermeneutical epistemology (containing explanations given by the actors of security / insecurity phenomenon).

This dichotomy is given by the impossibility to create complete axioms or formal theories as well as by the complete breakup with the empiricism. In other words, this dichotomy implies a combination of empirical assertions with axiomatic or formal rendering of security / insecurity phenomena¹.

Knowing security / insecurity, their nature and significance have certain implications or influences upon the practice of security (ensuring security).

The security doctrine is made up of beliefs, principles, and ideas in political, legal, security, religious domains etc. Thus, for instance, we find

¹ Valentin Stelian Bădescu, *Știința juridică românească și problemele ei actuale*, Studii și comunicări / DIS, Volumul XI/2018, p. 376.



the juridical doctrine syntagm; in the same manner we may speak about the phrase security doctrine, as well as that of philosophy of security / insecurity.

Furthermore, doctrine may also be considered a "*corpus of beliefs, principles, fundamental theses, models*"² of security. It may also comprise the scientifically proved opinions in the field of security / insecurity regarding the interpretation of security. Doctrine work in the domain of security means creating studies, monographs, handbooks, and scientific articles on security for clarifying concepts, conceptual correlations, theories, paradigms, etc.; obviously, security doctrine is marked by social, economic, political, environmental and military aspects of the respective time.

The concept lying under the security doctrine syntagm had to change in time and space due to the different evolutions from one state to another, from one age to another, and had therefore to undertake quantitative and qualitative mutations. In time, these mutations resulted in a distinctive approach aiming at the synthesis, systematization, analysis, and assessing depiction of security/insecurity, emphasizing its formal sources, the events and causes of insecurity, without ignoring sociological, philosophical, historic, juridical, cultural, medical, military, technical/technological aspects etc.

At the same time, it is focused on the practical issues raised by ensuring security in order to be analyzed / studied scientifically and generally, starting from particular events (from the particular-general relation) as acknowledging security cannot be limited to the level of empirical knowledge of insecurity events and the decisions made for ensuring security; nor can it be limited to general abstractions. Therefore, the objective of security doctrine is elaborating principles, laws, theses, and paradigms of security.

In domains of knowledge, sociology, and security, the security doctrine contributes, through coherence and synthesis, through precision and certain rational solutions for solving some security issues regarding human security, national security, regional security, international security etc., to citizens' trust in the rule of law, in democracy, in justice, in solving conflicts and crises. The general elements of security doctrine contain

² Valentin Stelian Bădescu, *op. cit.*, p. 372



certain standards of security, rationality, law, various theories among which that of logical argumentation, a philosophical view upon security in order to get as close as possible to the horizon of scientific knowledge of security. In addition, all the concept approaches of any security doctrine have to be subjected to the criticism of other researchers in the field, given the common morals of pluralist society. As morals cannot be considered as universal truth, it is fragmented, specific to human groups trying to take it out its relativity, its moral pluralism, in order for society to adopt "*a common moral attitude in essential issues*"³, including the issues of international security.

The dichotomy security doctrine / security science can be noticed in doctrine activity in the sense that in the field of security certain authors are tributary to the scientific paradigm that refers to acknowledging security centered on certain norms, certain security concepts, ethic/moral truth or state and non-state actors' behavior. In order to ensure security, each state has to pay greater attention to promoting the culture of security. In this sense, an important role is held by state institutions, mass-media, and civil society (including NGOs). By the culture of security, we understand all the values, attitudes (actions) and norms contributing to explaining concepts and making the members of society, on the one hand, understand the necessity of acquiring protection against threats and decreasing the risks to national security and, on the other hand, understand the concepts of Euro-Atlantic security, collective security, international security, etc.

Security education consists in developing the preventive attitudes of citizens in order to protect and defend themselves against threats, risks and vulnerabilities. The security education of citizens has special importance for keeping under control and monitoring both the evolution of internal and international security environment.

The culture of security implies activities of raising citizens' awareness regarding threats, risks and vulnerabilities to security so that they may be prepared and react accordingly in order to counter them. That is why mass-media, SRI and other institutions conduct periodic debates, workshops, conferences, round table discussions in which the main security issues are analyzed.

³ Valentin Stelian Bădescu, *op. cit.*, p. 375.



In the field of security there is a need for an own epistemological background, for schematized standards of security doctrine and new scientific approaches. The epistemological approach of security may contribute to the effort of going beyond the descriptive and normative science of security, by using axiological, praxiological, and even mathematical criteria in order to create a meta-theoretical reference theory / paradigm for security assertions (science) aspiring to a scientific character. According to epistemic (epistemological) pluralism, the scientific character has degrees and even versions in which the science of security *"has different hypostases and close relations"*⁴, as anticipated in the lines above. The essential issue here is the fact that scientific research in the field of security, which is a socio-humanistic discipline, the event / action of security / insecurity *"inevitably involves the observer himself"*⁵, and, moreover, within the security research / analysis ideological positions are adopted that might affect its scientific character. There were frequent exclusivist approaches noticed in the domain of security knowledge regarding explaining and comprehension, as well as the internal and external points of view. As security cannot be explained through itself, it is necessary to involve a larger number of perspectives. This issue that has to do with research regarding the security phenomenon requires a certain pattern of viewpoints: internal-external, understanding-explanations based on a meta-theory in which certain complex models might allow for correlating the language of security with the juridical (dogmatic) one and with that of social science which requires adopting epistemic (epistemological) pluralism through which to *"correlate the scientific virtual aspects of dogmatics"* of security and *"juridical dogmatics with the alternative practical virtual aspects proposed by social sciences"*⁶.

The epistemic approach of the "concept of integrating knowledge" allows going beyond the scientific specialization "understood as dogma" of security, for example in the situation in which "the quantitative approach" proclaims itself as "the only scientific one" in comparison to the qualitative one, "hegemony and colonizing knowledge".

⁴ Valentin Stelian Bădescu, *op. cit.*, p. 376.

⁵ *Ibidem*.

⁶ *Ibidem*, p. 377.



3. Formulating hypotheses of security

In 2003, the President of the United States launched the invasion of Iraq under the pretext that it had weapons of mass destruction. Ten years after that, Times wrote: *"The war in Iraq was not necessary, but rather costly and detrimental... It was based on flawed information manipulated to serve ideological purposes"*⁷. These were the causes of triggering the immense refugee waves that hit like a tsunami Western states. That is why we can now formulate the following security hypothesis for Western states: we either stick to the old paradigm "Si vis pacem, para bellum", or we pass on to a new paradigm: "Si vis pacem, para pacem" and we will have the chance of a lasting peace. Unemployment and economic, social, and political tensions in the European Union also influenced the behavior of Muslim minorities in those states (France, Germany, Spain, Italy, UK, etc.). This analysis results in the following hypothesis of security/insecurity: The more millions of Muslim emigrants in Western states, the more numerous and dangerous the terrorist attacks in those EU countries. Another way of putting it would be: If other millions of Muslims continue emigrating to Western states, then the national insecurity of these states is going to grow proportionally to the number of migrants per year.

In African and Middle East countries with a terrorist potential, the groups militating for the emergence of the new Caliphates take advantage of ethnic and religious conflicts, poverty, corruption, injustice, dictatorship, lack of education etc. for the purpose of directing and focusing frustration and hatred of some people on trans-border organized crime with the help of certain extremist / radical minorities. In 2015 and almost every year there were over 200 terrorist attacks, of which many were successful in the European Union. Some of these attacks included the use of explosives and thus, every year, there were over 100 killed and 1,000 people wounded.

The preparation of these terrorist attacks can be analyzed from several perspectives: geopolitical, political, economic, internal and external conditions etc. To this purpose we need to study a large quantity of data, information and especially events that have to be carefully investigated, in

⁷ Hendrik Willem van Loon, *Istoria omenirii*, traducere de Cornelia Dumitru, Humanitas, București, 2017, p. 653.



detail; for instance, violence can also be triggered by an internal economic crisis that is becoming acute.

Terrorism can also be characterized from the point of view of the political dimension of analysis (Table no. 1):

No.	CLASSIFICATION	MANNER OF ACTION AND PURPOSE
1.	State terrorism	Coercion acts of the state for social, ethnic, or religious repression of population
2.	Political terrorism	Assassinations with obvious political purpose
3.	Ordinary terrorism or banditry	Violent actions for obtaining material benefits without immediate political purposes

Table no. 1. Classifying terrorism from the point of view of political dimension

From the point of view of political involvement, different categories of terrorism may be identified (Table no. 2).

No.	CATEGORIES	PURPOSE
1.	State terrorism	Obstructing legal and social systems (coercions for holding on to power).
2.	Nationalist terrorism	Trying to set up a separate state for a national group (national freedom).
3.	Fundamentalist – religious terrorism (religious terrorism)	Imposing religious precepts (Christian Identity Movement Violent Salafist Movement, Shiite Extremism).
4.	Ideological terrorism	Imposing ideological concepts: Red Brigades; Sandero Luminoso, Nepalese terrorism; eco-terrorism etc.
5.	Extreme left terrorism	Destroying the capitalist regime and founding communism.
6.	Extreme right terrorism	Destroying liberal regimes and turning them in dictatorship systems.
7.	Anarchistic terrorism	Annihilating political leaders and destroying state authority.

Table no. 2. Classifying terrorism from the point of view of political involvement

According to the attack means used, there are several types / forms of terrorism (Table no. 3).

TYPE	MEANS
Regular	Firearms and side arms
With explosive means	Explosives placed in various vehicles, in drones, traps etc.



With CBRN means	Chemical, biological, radiological, or nuclear
With cyber means	Different IT systems targeting softs
With non-lethal means	Non-kinetic means

Table no. 3. Classifying terrorism according to possibilities of attack

If United Nations Organization manages to give a definition of terrorism that is universally accepted, then we will be able to approach the terrorist phenomenon from both the legal and legislative points of view.

Following careful examination (analysis) of history, the governments of certain states took political and diplomatic actions meant to strengthen peace and security. President Obama's speech in Cairo was meant to reconcile Americans with Muslims by re-examining the relation between them. He stated that the West and the Islam sometimes established cooperation relations while at other times they waged religious wars. He also said that instead of empowering those that incite to hatred, it would be preferable to place in positions of power those who promote cooperation, so that peoples of the world "*acquire justice and prosperity*" and "*this circle of suspicion and discord come to an end*"⁸.

Prime minister Kevin Rudd asked for forgiveness the aboriginals in Australia, in 2008, as these people had been banished from their lands.

*"We are asking for forgiveness from mothers, fathers, brothers and sisters for destroying families and communities. And we are asking for forgiveness for the humiliation and prejudice caused to a proud people and a proud culture"*⁹.

Hence, we may talk about the following assumption of security/insecurity: in case of groups of people that have common / overlapping interests, there will either be dialogue, mutual respect and cooperation or strife, hatred, crises and conflicts.

The American stock market crashed in the United States and then in Europe and there was global recession in 2008. So, the recession of American economy was the cause of world recession and the main cause was the mortgage crisis, namely the loan offered by American banks to

⁸ Hendrik Willem van Loon, *Istoria omenirii*, translation by Cornelia Dumitru, Humanitas, București, 2017, p. 652.

⁹ *Ibidem*, p. 654.



those who purchased a house and then, throughout the next years, they had to reimburse that mortgage. The issue was caused by the fact that banks offered credits with a high degree of risk, namely to people who were not capable of returning the loan (and were therefore not eligible for being given that loan in the first place).

In 2007, when the price of lodgings rose and the economic decline began, the owners could no longer pay their debts to the banks and thus, the banks confiscated millions of lodgings. Something similar happened in Europe, too. There was a huge uprising and people started to ask for measures against those who were guilty of stealing their economies stored in banks, because of the highly risky speculations practiced by bankers. States' governments started to provide substantial help to banks and investment firms that were to blame for the emerging crisis but did not help the millions of people whose houses had been confiscated.

The affected people gathered in massive protest on Wall Street as the reasons/causes that had triggered Great recession (global economic-financial crisis) were the same that had caused in 1929 the Great Depression, namely the enormous difference between the fortune held by a handful of wealthy people and the vast majority of people. Protests of this kind happened everywhere in the world and protesters asked for banking regulation which would have meant that bankers were not allowed to make banking speculations and were instead compelled to abide by certain rules of safekeeping the savings of citizens in their banks.¹⁰

The lines above lead to the following security assumption: If there is no law regarding banking regulation, such as for instance Glass-Steagall Law promulgated by American President F.D. Roosevelt, then the Great Depression or Great recession will happen all over again just as it happened between 1929 and 1933 and between 2008 and 2009. This assumption was valid between 1929 and 1933 and was then confirmed after 75 years, as if a banking experiment had been performed by mentally deranged scientists.

The huge difference between the theory of security / insecurity and the reality / practice of security has to be well-understood in order to understand

¹⁰ Hendrik Willem van Loon, *Istoria omenirii*, translation by Cornelia Dumitru, Humanitas, București, 2017, p. 654.



the differences between the state of war and the illusion of peace in the minds of certain rulers or dictators such as Stalin.

Sometimes, the practice of security / insecurity can only be understood through a holistic approach. Thus, for instance, the events that happened at the western border of Soviet Union in 1941 and in Stalingrad (Volgograd) between September 1942 and January 1943 cannot be correctly perceived through a usual analysis of security or through a simple military analysis (exactly because they were extraordinary battles of the Second World War). The complex reality of the battle in Stalingrad cannot be perceived only by resorting to the arguments brought by Military Science (be it German or Soviet), but also through the arguments brought by the science of security / insecurity – a trans-disciplinary science that comprises ideas taken from sociology, psychology, history of security, political science etc.

"Thus, for instance, Stalin and his ambassador in Berlin were convinced a few days and even a few hours before the war, that this was a mere act of disinformation, although the military attaché in Berlin informed the ambassador that 180 German divisions were in formation at the Western border of USSR. The dichotomy between reality and confidence/perception, between peace and war, between security and insecurity is sometimes absolutely huge. Moreover, there is a great difference between the large amount of information, coming from German officials, regarding the imminence of war started by Hitler and Stalin's conviction that everything is just disinformation. It is amazing to notice the sheer stupidity of Stalin and his ambassador in Germany who, two weeks prior to the war, were informed by the German ambassador in Moscow (Count von Schulenburg) that Hitler was planning to attack the USSR in two weeks' time (June 22nd, 1941, 3:00 a.m.).

Although Soviet border troops reported that thousands of tanks were stationed beyond the border with their engines already started, that the barbed wire network was destroyed and the commander of Kiev special region reported that War was going to start right away, Stalin did not believe those reports and said that it was only an act of disinformation. Two or three days after the war started, Stalin held a meeting with Beria and Molotov and asked them if it would not have been better to make peace with Hitler and give up a large part of Belarus and Ukraine as well as the Baltic



states? The Bulgarian ambassador who was asked to play the role of go-between, refused as he considered that even if the Red Army were to retreat up to Ural Mountains, it would still "eventually win the war". The huge majority of Soviet citizens, during the first days of war, had no idea about the USSR being invaded by German troops, which proves the cleavage between the indoctrination of population by Stalin's communist propaganda and the Soviet leadership completely subject to the orders given by him.

Based on this analysis, we may formulate the following security assumption: If and only if a dictator is intelligent enough and has the theoretical and practical leadership skills (including those required by a military leader), he will be able to skillfully use in an opportune manner the information received in order to make the difference between the state of war and the dissuasion of peace between the outburst of the war.

4. Conclusions

The history of security (that part of history referring to events that are connected to security/insecurity) may constitute a source of security / insecurity assumptions, that have various degrees of generalization or abstracting, and some security assumptions may be deduced logically only through the researcher's reasoning mechanism, while others stem from empirical research and may be verified directly. The science of security requires that security assumptions be verified empirically, if possible, by resorting to historic reality.

The results obtained from historic data may support (confirm) or deny the initial assumption. Assumptions can be made by using various connective phrases: "Either... or... ", "If..., then... ", "The more... the more...", etc. For instance: either this or the other one is true.

There are different ways to confirm or invalidate an assumption: comparison, explanation, comprehension, quantitative and qualitative methods, demonstration, argumentation etc.

Within the security science, we may use the following methods: document analysis and observation, that has a large epistemic opening (qualitative observation is used when we investigate a complex phenomenon, such as the security / insecurity phenomenon).

Examples of security assumptions:



- We either have dialogue, mutual respect, and cooperation, or we will have strife, crises and conflicts.

- We either stick to the old paradigm “Si vis pacem, para bellum”, or we move on to a new paradigm “Si vis pacem, para pacem” and we will have the chance of a lasting peace.

Bibliography

1. Bădescu, Valentin Știința juridică românească și problemele ei actuale, Stelian Studii și comunicări / DIS, Volumul XI/2018.
2. Bădălan, Eugen; Bogdan, Vasile Organizații și structuri de securitate, București, 2016.
3. Bădălan, Eugen; Savu, Gheorghe; Botoș, Ilie; Bogdan, Vasile Tratat de criză teroristă, Editura militară, București, 2011.
4. Mișu, Ștefan Omenirea secolului al XXI-lea și guvernul mondial, Editura RAO, 2011.
5. Van, Loon; Willem, H. *Istoria omenirii*, translation by Cornelia Dumitru, Humanitas, București, 2017.
6. * * * Institutul de studii și cercetări ale terorismului, Revista TERORISMUL AZI, Vol. XXVIII- XXXIII, an III, 2008.



INFORMATION WARFARE - AN OBJECTIVE OF NATIONAL SECURITY

Colonel (ret.) Professor, Gheorghe BOARU, PhD

Tenured member of the Academy of National Security Sciences,
Tenured member of Academy of Romanian Scientists,
E-mail: boarugheorghe@yahoo.com.

Abstract: *The approach to the information warfare topic can contribute to the definition and promotion of national security objectives and the empirical and scientific results of extended security analyzes in the context of Romania experiencing a turbulence, uncertainty and diffusion of complex security states in the eastern flank of NATO, the convergence of the North-South and East-West security and insecurity axes.*

National security may be the predilection target of the informational war, conducted by adversaries and hostile forces (groups) in times of peace, in crisis situations and especially in the case of military conflict.

In this article, I wanted to highlight the existence of "think-tanks" in the field of information warfare in the West as well as in the East. I supposed that we are equally interested in the concept of "the West", because we are members of NATO and the "East" conception because we are neighbors with Russia who developed the concept of information warfare and even applied it.

Keywords: *Information warfare; information operations; informational superiority; information; national security; information and communications technology.*

Introduction

Romania is in a period of turbulence, uncertainty and diffusion of complex security states in the eastern flank of NATO, the convergence of the North-South and East-West security and insecurity axes.

I believe that addressing the issue of informational warfare can help to define and promote national security objectives and the empirical and scientific results of extended security analyzes.

The more current the issue is that, in response to one of the objectives of the National Defense Strategy of the country in force, the



strategic objectives of national defense are established on the basis of their provisions and respond to the need to promote national interests, combat asymmetric threats, risks and diminishing internal vulnerabilities.

One of the objectives of the National Defense Strategy of the country, established according to the requirements of the National Security Strategy of Romania, is to increase the specific contribution to ensuring regional security and stability. According to this document¹, Romania is involved in regional security and stability on the following complementary levels:

- Participation in the process of defining and implementing NATO's and the European Union's Stabilization, Co-operation and Security Policies in Central, Eastern and Southeast Europe;
- Strengthening the role of stability and security provider in the Balkans, in the wider Black Sea area and in the ex-Soviet space.

I believe it is important and useful to publish some aspects of the informational war based on previous personal studies and personal journalistic activities and on the conclusions of my own studies in this field as well as to highlight the opinion of some representatives of "think-tanks" from both the "West"² as well as in the "East"³. Perhaps we are equally interested in the conception of "the West," because we are NATO members and the "East" conception because we are neighbors with Russia that has proliferated various threats to Romania⁴.

¹ HG nr. 30/2008 privind aprobarea Strategiei naționale de apărare a țării, cap. 2.4.

² Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, Washington, D.C.: CCRP Publication Series, August 2001; Cebrowski, Vice Admiral Arthur K., John J. Garstka, "Network Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings*, January 1998; Martin C. Libicki, *What Is Information Warfare?*, 1995.

³ *Игорь Панарин, *Первая мировая информационная война. Развал СССР*, Санкт-Петербург: Издательство «Питер», 2010;

**Jolanta Darczewska, *The anatomy of Russian information warfare. The Crimean operation, a case study*, Publisher: Ośrodek Studiów Wschodnich im. Marka Karpia, Centre for Eastern Studies ul. Koszykowa 6a, Warsaw, Poland, MAY 2014, p.14 /The Panarin school, p.17/The Dugin school;

***Дугин Александр, *Русская война*, Москва, ТД«Алгоритм», 2015.

⁴ *Russia threatens openly Romania!* Unprecedented tensions come from Moscow after the head of Russian diplomacy, Sergei Lavrov, recently launched an unprecedented attack on NATO, and implicitly Romania, talking about the risks involved in installing anti-ballistic



Also, the case of Ukraine with the phenomenon "Euromaidan" - and the annexation of Crimea (2014) are two examples worth studying and analyzing.

In this context, I have proposed to publish more articles on this subject.

Informational warfare - a war without frontiers

The characteristics of the armed struggle have fundamentally changed, its violent character being replaced by nonviolent or less lethal forms of action. The modern information society, based on the unprecedented development of information and communication technology, which has profoundly transformed all areas of activity, has led to important changes in the war as well, and now it is becoming mostly informational.

Information has become one of the nation's main riches and the struggle for it is the basic means of neutralizing the enemy, as without safe and continuous information, national security and effective military action can not be ensured.

Informational superiority has gained much greater importance than it had previously been aerial, terrestrial or maritime superiority, and is the main purpose of the action taken.

The informational warfare is a multilateral approach to the present, which repels all sorts of borders, based on offensive and defensive actions (like any other war), which take into consideration a multitude of forms of attack of information and information systems with disastrous impact on the adversary's decision-making and action processes.

As a main element guaranteeing the existence and multilateral development of states, national security could not be the predilection target of the informational war, conducted by adversaries and hostile forces (groups) in times of peace, in crisis situations, and especially in the case of military conflict.

American systems in Europe. [<https://www.capital.ro/rusia-ameninta-romania.html>] accessed on 20.02.2019.



The forms of action of the informational war on national security are numerous and of great complexity, which can cause its very profound damage in the medium and long term, by decommissioning the main elements of the information systems, namely the sources of information gathering, communications and computers, acting concurrently on their staff and the decision-making structures of the country.

In this context, the defensive information actions, which will be carried out continuously, must ensure the protection of the information and information systems regarding the national security, which is the fundamental condition for the efficient management of all fields of activity.

The subject is always present, because the international environment itself, the global environment, the security state of states are in a permanent transformation, important events of contemporary geopolitical change, often coming out of the plan of analytical prediction.

Informational warfare - evolutions

One of the greatest strategists of history, Sun Tzu, the Chinese philosopher who lived around 500 BC. wrote: "Know the enemy and know yourself; in one hundred battles you will never be in danger. When you do not know the enemy, but you know yourself, your chances of winning and losing are equal. If you are also unaware of the enemy and yourself, you will certainly be in danger in every battle. "

The concept of warfare in this sense has not changed, but only the means and speed of information acquisition and transmission have changed.

According to Alvin and Heidi Toffler, the wars of today's era are part of the category "third wave", wars of information society called "Aero-Terrestrial Fights" and states that the military operations of the Persian Gulf War represented "the end of the industrial age war and the beginning of the informational age war".

The "Storm in the Desert" operation gave the Pentagon a first idea of the war of the future. Combining electronic warfare, command and control warfare, and psychological operations, the coalition launched an attack against the Iraqi intelligence system that hastened the end of the conflict.

The Persian Gulf War used the most misleading use of information and the information war. The flow of information sent and received on the communications channels did not leave on the members of the coalition any



rest periods: 700,000 phone calls, 150,000 messages in 24 hours, managing 350,000 frequencies and controlling 2,240 daily AWACS planes.

James Adams points out, in one of his works, that "... many lessons have been and will be detached from the Storm in the Desert. Some are not new; others yes. However, one is fundamental: the nature of the war has changed dramatically. The fighter who wins the information campaign defeats ... information is the key to modern war - from a strategic, operational, tactical and technical point of view⁵".

Analyzing Romania's military efforts to integrate into European and Euro-Atlantic structures, it is impossible not to admit that at present, Romanian military thinking faces a major challenge: identification and decipherment, from a perspective information technologies, the consequences of changes in the areas of understanding the notions of "security", "war", "military operations", "threat", "conflict space" and the examples could continue⁶.

The information warfare involves taking steps to degrade or manipulate an opponent's information systems, while actively protecting their own. In the coming decades, the threat to information systems will increase, thus increasing the need for security at the same pace as the development of information systems and threats to them.

Between 1990 and 1992, the disappearance of the bipolar system led to significant discontinuities in NATO's military thinking and strategy, triggering the search for new tools and the need to redefine security objectives, which led to the emergence of the concepts of Information Warfare and Information Operations.

At least three grounds underlie the development of these concepts⁷:

- accepting the Informational War as a "political war" as a component part of a state's policy for both promoting and protecting national interests, ensuring at the political level opportunities for "peacetime aggression";
- the threat with nuclear respond, even flexible, is no longer represent a

⁵ ADAMS JAMES, *Următorul – Ultimul război mondial*, Ed. ANTET, București, 1998, p.109.

⁶ Col. prof. univ. dr. Gheorghe BOARU, *RĂZBOIUL INFORMAȚIONAL ȘI OPERAȚIILE INFORMAȚIONALE*, Editura Universității Naționale de Apărare, București, 2004, p.3.

⁷ Col. prof. univ. dr. Gheorghe BOARU, *RĂZBOIUL INFORMAȚIONAL ȘI OPERAȚIILE INFORMAȚIONALE*, Editura Universității Naționale de Apărare, București, 2004, p.4.



credible deterrent of an aggression, in the condition of the bipolar system's disappearing;

- Operations other than war impose at tactical level the use of precise and limited non-lethal forces which, in order to obtain minimal losses, require another type of tactics, centered on timely information, called info-tactics.

A short history

The first conceptual concretisation began in 1976 when Dr. Thompson P. Rona⁸ wrote a report entitled "Weapon Systems and Information War" for the Boeing Company he was working on, in which he used, for the first time, the term of informational warfare.

Dr. Rona pointed out that information infrastructure has become a key component of the US economy. At the same time, it becomes a vulnerable target both during the war and during the peace period.

With regard to the US Army, the USAF (United States Air Force) began to actively discuss this issue in the 1980s. Until then, it was agreed that "information" could be a target and could also be used as a weapon.

In initiating the study and analysis of the field of information warfare, I started from the idea that information was, is and will be the key element of all informational processes.

In a specialized scientific paper it is stressed that "... in the analysis of a military informational activity, information can be considered as "raw material", "purpose", "target", "weapon" and its protection is even more important and more complex⁹".

In 1985, a 25-year-old Chinese young man, Shen WeiGuang, wrote an essay titled "War of Information." In this paper he talked about notions such

⁸ **Thomas P. Rona** worked in Seattle, Washington for Boeing between 1959 and 1984. Subsequently, Dr. Rona held various positions including the Special Assistant for Space Policy in the Department of Defense, 1984-1986 and Deputy Director for Government Programs within the Office of Scientific and Technological Policy at the White House from 1986 to 1987. In 1987, President Ronald Reagan nominated him as Associate Director of the Office of Science and Technology. In 1989, he became Scientific Advisor to President George H.W. Bush. He has elaborated several works in the field of informational warfare.

⁹ Gheorghe BOARU, Iulian Marius IORGA, *SECURITATEA SISTEMELOR INFORMAȚIONALE MILITARE*, Editura Universității Naționale de Apărare „Carol I”, București, 2018, p. 6.



as "the border of the information", "information factory", "informational army", "police of the informations ", "home struggle", and described information as an all-encompassing feature of society.

Shen WeiGuang became senior officer in the Chinese army and had some professional views on the information war, such as: "China has realized that it could not threaten countries as a superpower that could cope with the current nuclear power, but it can do with his force IW (Information War). For example, China may theoretically threaten the financial stability of the United States through IW in peacetime. Electrons are at the heart not only of the IW, but also of the global economic explosion associated with stock markets and e-commerce. Characteristics of information (global coverage, speed of light transmission, non-linear effects, inexhaustible, multiple access, etc.) control the material and energy of the war in a way that nuclear weapons can not"¹⁰.

In another work in the same field states that *"The objectives of the first attack will be the computer networking system connecting the political, economic and military institutions of a country as well as society in general, as well as the ability to control decision making for prevent coordinated actions. This requires both attacking cognitive and informational systems"*¹¹.

This emphasis on IW implies that not only military will lead in the future war, but also civilians. Some Chinese theorists¹² have recommended the organization of special warfare detachments and computer experts to form a shock brigade of "network warriors" to carry out this task. They will

¹⁰ Shen Weiguang, *Focus of Contemporary World Military Revolution—Introduction to research in IW,* Jiefangjun Bao, 7 November 1995, p. 6 as translated and reported in FBIS-CHI-95-239, 13 December 1995, pp. 22-27; https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf.

¹¹ Shen Weiguang, *Checking Information Warfare-Epoch Mission of Intellectual Military,* Jiefangjun Bao, 2 February 1999, p. 6 as translated and downloaded from the FBIS web site on 17 February 1999.

¹² Li Yinnina, in Huang Youfu, Zhang Bibo, and Hang Song, *"New Subjects of Study Brought about by Information War—Summary of Army Command Academy Seminar on „Confrontation of Command“ on the Information Battlefield"* Jiefangjun Bao, 11 November 1997, p. 6 as translated and reported in FBIS-CHI-97-354, insert date 23 December 1997.



look for critical nodes and control centers on networks and will sabotage them.

The first comparable works of Western military thinkers emerged only in the early 1990s.

French writer of Russian origin Vladimir Volkoff wrote in 1998 about the informational war:

*"Becoming aware that in the modern world, everything translates into information, the Americans have established the first theory of information warfare. In the United States there are proliferating military and civilian institutions that deal with this issue"*¹³.

Also in the work of the same author there is a logical statement about one of the forms of informational advantage - the informational dominance: *"Technology makes it appear new applications every day, and the American society has adapted itself more quickly, the more the sharing of information is an instrument of economic and political power. From this revolution came the concept of informational domination, according to which it is possible to master the environment by mastering the information"*, as David Bouden¹⁴ writes.

In 1999 Rémi Kauffer¹⁵ concludes that *"... therefore the Americans have made an advance in InfoWar, a term that designates the war of information"*¹⁶. The term is relatively recent and includes several complementary categories. Initially, simple information, then superinformation, intensive bombardment of the media, decision-makers and the public with a wealth of data generally favorable to those who emit them appears. Follow counter-information, which combines art and defense by dismantling the opponent's arguments with objective and verifiable elements.

Misinformation complements the panoply. This technique involves an orchestrated, sustainable action as well as constant technical, financial and human means.

¹³ Vladimir Volkoff, *TRATAT DE DEZINFORMARE* - De la Calul Troian la Internet, Editura ANTET, p. 210.

¹⁴ David Bouden, apud Vladimir Volkoff, *op. cit.* p. 210.

¹⁵ Rémi Kauffer is a journalist (Figaro, Historia, ...) specializing in contemporary history. He wrote with Roger Faligot many books on secret services and information services. He is also a lecturer at the Institute of Political Studies in Paris, the Economic War School and the Catholic Institute for Higher Education.

¹⁶ Rémi KAUFFER, *Guerre économique L'arme de la désinformation*,. Grasset, 1999.



Henri Pierre Cathala publishes a work¹⁷ he names, symbolically, "The Age of Disinformation," analyzing the general traits of this profoundly antisocial act, as well as its forms of manifestation. Disinformation, Henri-Pierre Cathala tells us, belongs to the "art of the detour". She is always deliberate, premeditated, and counts on subversive actions,

in order to confuse the opponent, victimizing him, be it a political personality, or a social group, state or society. Misinformation is a form of manipulation. This work has been republished by several publishers.

Parents of the informational war can be considered the psychological warfare (propaganda, psychological operations, psychological actions, ... whatever I call them) and the electronic war.

In a war, the psychological struggle is set on three levels: - Deciders (commanders); - Own and adverse bands; - Public (own, adverse, neutral).

Perhaps the first to say that was T.E. Lawrence¹⁸: *"It was a more subtle than tactical and worthy of being done, because it had to deal with uncontrollable factors or individuals unable to receive a direct order.*

We had to prepare our minds for the battle, with the same care and precision as the officers had prepared their bodies. and not only the minds of our people, though they certainly came first.

We should also prepare the minds of our enemies, as long as we can reach them; and then the other minds of the nation that support us behind the front, because more than half of the battle was going on there, backwards.

*Then the minds of the enemy nation who await the verdict; as well as those neutral who were standing and watching. All, one by one"*¹⁹.

¹⁷ Henri Pierre CATHALA, *Epoca dezinformării*, Ed. Antet, 2000; Cathala, Henri-Pierre, *Epoca dezinformării*, Ed. Militara, Bucuresti, 1991.

¹⁸ Thomas Edward Lawrence, also called Lawrence of Arabia, was the name given to an British intelligence officer who fought alongside Arab Guerrilla forces in the Middle East during the First World War.

¹⁹ T. E. LAWRENCE, *Seven Pillars of Wisdom: A Triumph*, Oxford University Press, 1926. Seven pillars of wisdom represent the autobiographical story of the experiences of British soldier T. Lawrence ("Lawrence of Arabia") while serving as a liaison officer with the rebel forces during the Arab Rebellion against the Ottoman Turks from 1916 to 1918.

The work was completed in February 1922, but was first published in December 1926.

Seven pillars of wisdom represent the autobiographical story of the experiences of British soldier T. Lawrence ("Lawrence of Arabia") while serving as a liaison officer with the rebel forces during the Arab Rebellion against the Ottoman Turks from 1916 to 1918.

The work was completed in February 1922, but was first published in December 1926.



Theoretical Perspectives of the Informational Warfare

Although the Informational War has been intuited and conceptualized since 1976 by Thomas P. Rona, awareness of the possibility of a different war, an invisible war, much subtler than the classic war, has only been realized very recently, the tone being given by the military environment.

One of the first building blocks of the concept of Information War was A. Toffler's "Third Wave" book, published in 1980. In this book one can read: "To attack a nation can obstruct the flow of information - cutting off the link between multinational company headquarters and its foreign affiliates, lifting information barriers around it, etc. The international vocabulary was enriched with a new expression: "the sovereignty (supremacy) of information".

One of the first building stones of the concept of Information War was A. Toffler's book, *The Third Wave*, published in 1980. In this book can be read: ... "to attack a nation can obstruct the flow of information - cutting the link between the headquarters of the multinational society and its foreign affiliates, the raising of informational barriers around it, etc. The international vocabulary was enriched with a new expression: "the sovereignty of information".

This reflection on the informational age was continued by another book by the same author, entitled "War and Anti-War", which allowed the debate in the United States to relaunch the concept of Information War.

The US Department of Defense, which has pursued these reflections and has, to a large extent, provoked them, has gone through several stages, from the concept of Manoeuvre Warfare, applicable to a conventional war on Strategic Information Warfare. This is a global concept that covers at the same time the notion of Conventional Warfare, which mainly targets the economic infrastructures of the opposing state, the notion of Command & Control Warfare, which classically looks at the destruction or neutralization of the adverse military forces and the notion of Information Warfare.

The expression "Information War" covers a whole series of meanings. The lack of a clear definition of the Information War is visible in all the literature. So far, it has been attempted to define the origins of this type of war, but no one has yet established its principles. Almost every person who writes about the Informational War is confronted with this



difficulty. Of course, there have been several definitions that resemble each other. But the fact that almost everyone writes about the Informational War feels compelled to define it, emphasizes this lack of a universally accepted definition.

The information war theory and practice has lately been receiving increasing attention from politicians, strategists, scientists and the mass media in various countries, especially from North Atlantic and European space, a phenomenon easy to find in pursuing frequency of public discourse, conferences, symposiums, books, studies, and articles addressing this issue.

The "hot" subject matter is also revealed by the diversity and exoticism of some concepts ("critical information infrastructure", "information operations"), university specializations (cybernetic strategy), institutions (Information Management College) ("hacker", "cracker"), all associated with the field of Information Warfare.

In the opinion of an author of works in this field, it is appreciated that *"Although there is no universally accepted definition, one can speak of the Informational War as a new form of war, considering the tools it uses to achieves the goals (thanks in particular to the explosion of information technology). It is important, however, to note that information technology not only allows the development of modern war but adds a new dimension to conflicts"*²⁰.

The information infrastructure, by its content and the technologies that make up it, is now considered an object of an informational war but also subject with the same strategic complexity as the traditional dimensions (aerial, terrestrial, maritime and spatial). Informational networks form a new battlefield, and information itself becomes a target. Each became separately, but also in combination with the others, both a weapon as well as the target.

At the same time, the Informational War can be said to be an old form of war, if reference is made to the concepts it is based on (Chinese philosopher Sun Tzu spoke 25 centuries ago about "cunning", about the art of deceiving the adversary, the need to prevent the opponent from properly assessing a situation. In a similar way, Machiavelli expressed himself in the

²⁰ Col. prof. univ. dr. Gheorghe BOARU, *RĂZBOIUL INFORMAȚIONAL ȘI OPERAȚIILE INFORMAȚIONALE*, Editura Universității Naționale de Apărare, București, 2004, p. 26.



fifteenth century when describing in the "Prince" or in the "Art of War" the qualities of the state man, the Prince, above all, he is a military leader who must have a selfish, calculated, cunning nature etc.).

As I have already mentioned, *"Information warfare is not a new practice in terms of the concepts after which it is guided. Aspects that could be considered as part of an informational war can also be identified during the Second World War (misinformation, intimidation, etc.). But the novelty that it brings today is the inclusion of sophisticated technical means in a global strategy, achieved according to the intended purpose"*²¹.

This strategy seeks to gain an advantage, an informational superiority over opponents or even allies.

Here are some arguments that mark the major differences between the historical role of information and current theories of information warfare:

➤ Possession of informational superiority was a problem of luck rather than system. Today, the Informational War depends on superior and systematic exploitation and timely dissemination of information.

➤ Information could influence some war plans, but not their execution. R.I. requires an early warning and decisions in a fast and changing battlefield.

➤ The wars were won or lost with or without information. Today information is paramount, and an Information War requires a safe flow of it.

➤ Communication channels were exposed to interception in the past. Nowadays, digital technology is extremely vulnerable to banning access to data manipulation attacks. Software attacks may not destroy weapons or forces, but they can certainly forbid them or immobilize them.

Synthesizing, the verbs that best fit to summarize the concept of Information War are: capturing/collection, transmitting, quickly processing information, preventing (opponent/ally doing the same), distorting, disinforming.

²¹ Col. prof. univ. dr. Gheorghe BOARU, *RĂZBOIUL INFORMAȚIONAL ȘI OPERAȚIILE INFORMAȚIONALE*, Editura Universității Naționale de Apărare, București, 2004, p. 27.



Conclusions

Information warfare is a modern form of action on states, especially on infrastructure for national security, which can seriously affect their economic and military power.

The emergence of this category of war is the result of humanity's transition to the information society and knowledge, based on the scientific revolution in all fields of activity, especially in information and communications technology, which determined that distances are no longer important for the realization of the communications on the whole Earth globe. As a result, some forms of the informational warfare may take place far from the attacked country, in perfect anonymity and with minimal risk.

Their use determines the disappearance of clear demarcation between peace periods and situations of crisis or military conflict, and the information attack can be executed in any of these.

However, it is to be expected that the intensification of the informational war will take place in crisis situations and especially during the conflict itself, which it requires it to be included as the main threats to the national security and defense capability of the country.

The situation is aggravated by the fact that, for now, information aggression is not subject to any international regulation, and can not be legally sanctioned and sanctioned by supra-state bodies.

Of course, being conscious of the serious consequences of the informational war, our country must be able to defend itself against it, as well as to use it if needed, especially in the case of military conflict, acting in accordance with the general principles of NATO's riposte.

Bibliography

1. * * * HG nr. 30/2008 privind aprobarea Strategiei naționale de apărare a țării. Publicat în Monitorul Oficial, Partea I nr. 799 din 28/11/2008.
2. Adams, James *Următorul – Ultimul război mondial*, Editura ANTET, București, 1998.
3. Gheorghe, Boaru, Iulian, Marius, Iorga *SECURITATEA SISTEMELOR INFORMAȚIONALE MILITARE*, Editura Universității Naționale de Apărare “Carol I”, București, 2018.



4. Col. prof. univ. dr. Gheorghe, Boaru *RĂZBOIUL INFORMAȚIONAL ȘI OPERAȚIILE INFORMAȚIONALE*, Editura Universității Naționale de Apărare, București, 2004.
5. Cathala, Henri-Pierre *Epoca dezinformării*, Editura Antet, 2000.
6. Cathala, Henri-Pierre *Epoca dezinformării*, Editura Militară, București, 1991.
7. Jolanta, Darczewska *The anatomy of Russian information warfare. The Crimean operation, a case study*, Publisher: Ośrodek Studiów Wschodnich im. Marka Karpia, Centre for Eastern Studies ul. Koszykowa 6a, Warsaw, Poland, MAY 2014, p.14 /The Panarin school, p.17/ The Dugin school.
8. Дугин, Александр *Русская война*, Москва, ТД «Алгоритм», 2015.
9. Rémi, KAUFFER *Guerre économique L'arme de la désinformation*, Grasset, 1999.
10. T. E., LAWRENCE *Seven Pillars of Wisdom: A Triumph*, Oxford University Press, 1926.
11. Игорь, Панарин *Первая мировая информационная война. Развал СССР*, Санкт-Петербург: Издательство «Питер», 2010.
12. Vladimir, Volkoff *TRATAT DE DEZINFORMARE - De la Calul Troian la Internet*, Editura ANTET.
13. Shen, Weiguang *Focus of Contemporary World Military Revolution - Introduction to research in IW*, Jiefangjun Bao, 7 November 1995, translated and reported in FBIS-CHI-95-239, 13 December 1995.
14. Shen, Weiguang *Checking Information Warfare-Epoch Mission of Intellectual Military*, Jiefangjun Bao, 2 February 1999, translated and downloaded from the FBIS web site on 17 February 1999.
15. Li Yinnina; in Huang Youf; Zhang, Bibo; Hang, Song; *New Subjects of Study Brought about by Information War—Summary of Army Command Academy Seminar on “Confrontation of Command” on the Information Battlefield*, Jiefangjun Bao, 11 November 1997.
16. * * * http://www.dreptonline.ro/legislatie/hg_strategie_nationala_aparare_tara_30_2008.php.



17. * * * https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf.
18. * * * http://publ.lib.ru/ARCHIVES/P/PANARIN_Igor'_Nikolaevich/_Panarin_I.N..html
19. * * * <https://www.capital.ro/rusia-ameninta-romania.html>.



HYBRID WARFARE AND THE MARITIME COMPONENT. TOGETHER OR AS SEPARATE ENTITIES?

Brigadier General (ret.) Professor Viorel BUȚA, PhD
Tenured member of Academy of National Security Sciences,
Tenured member of the Academy of Romanian Scientists,
E-mail: vbuta49@yahoo.com

Lieutenant (Navy) Andrei PAVĂL, PhD student
Fleet Command, Navy Staff,
E-mail: pavalandrey@yahoo.com

Abstract: *More and more actions carried out by different state or non-state actors are associated by the international scientific community with the latest generation warfare, namely the hybrid warfare. Moreover, the defining elements for hybrid warfare are specific to the land component, but lately, they have become noticeable in the naval domain, the maritime component playing a quite important role in carrying out hybrid actions.*

The "mutations" undergone in time by this type of threat, as a result of globalization and technological expansion in the IT field, force the maritime component to permanently adapt to the new types of threats and seek to contribute to counteracting and conducting actions specific to the hybrid warfare.

The scientific community must place this type of threat in a certain pattern in order to perform adequate research and develop unitary countermeasures that can be taken at the tactical level as well as the operational-strategic level where the political factor plays a significant role.

Keywords: *hybrid warfare, maritime, naval forces, naval power.*

The concept of "hybrid warfare" started being debated in the academic environment long before the annexation of Crimea by Russian Federation in 2014, an act that was largely criticized at the level of international community. The annexation of Crimean Peninsula, at that moment part of Ukraine, gave rise to a lot of controversies worldwide, at the same time relaunching debates on hybrid warfare, the lesson taught by Russian Federation to the whole worlds coming at a time when attention was focused on other hot spots on the globe, the "frozen conflicts" in the Extended Black Sea area being somehow faded in the background.



Defined as a new type of warfare, or 4th generation warfare, hybrid warfare is characterized by harmonization and synchronization of military operations with various non-military actions and directions, applied gradually, both at cultural, social, humanitarian, economic levels and at political, diplomatic and strategic levels on the entire spectrum of conflict, corresponding to the elements it comprises¹.

Although more than five years have passed since the results obtained after applying, one by one, all the elements involved in waging hybrid warfare, the international scientific community has still not reached any consensus regarding a clear definition of hybrid threat to the international geopolitical actors.

In the academic and analytical environments, this type of warfare is not new, as it has suffered certain "mutations" along the years, depending on the new and diverse aspects implied by its defining elements which are going to be briefly presented in this article.

The concept was initially introduced by military theorist Evgheni Messner, colonel in the Tsarist Army General Staff during the two World Wars, who coined the phrase "meatejevoina" ("insurgency war" or "insurrection war").

Thus, the inter-war period witnessed the birth of a new type of warfare, created and developed by Bolsheviks with the clear purpose of challenging and ultimately defeating the West² by ousting an existing political regime or an army of occupation without resorting to direct military confrontation³.

Along the years, this phenomenon has suffered a series of changes that made the transition to insurrection warfare and then to what is nowadays known as hybrid warfare and the shapes it takes within military disputes. A turning point in the genetic modifications of the new generation warfare was year 1965, when the Defense Advanced Research Projects Agency – of the Department of Defense (DoD) in the USA created the first network of interconnected computers under the name of ARPAnet, network

¹ Buța Viorel, Valentin Vasile, *Războiul de tip nou: perspectiva Rusă*, Gândirea Militară Românească, issue 2 of 2015.

² Florina Mihaela Nicolescu, *Războiul hibrid. Perspectiva conceptuală rusă*, accessed on 15.09.2019, at <https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa>.

³ Academia Română, Institutul de lingvistică „Iorgu Iordan – Al. Rosetti”, *Dicționarul explicativ al limbii române*, Editura Univers Enciclopedic, București, 2016, p. 561.



which afterwards turned into today's Internet, with its well-known challenges and risks to security and stability at regional and world levels.

After that, during mid '2000s, the theoretical version of the concept, initiated by a former American Navy officer, Frank G. Hoffman, brought into discussion and systematized the new forms of aggression in the international system. Combating methods and mechanisms in politics, economy, military counter-intelligence, cyber environment, fake news etc., meant to discredit governments and institutions, destabilize societies or influence elections, nowadays make the use of military force only a matter of last resort. In turn, Russian experts tried to support their inverted claim that the West is carrying out a "hybrid endurance warfare" against the Russian Federation⁴.

Analyzing the evolution and transition of hybrid warfare from the inter-war period until the present time, we could pick up its main characteristic, namely the lack of use of armed force, which makes it unique and worthy of analysis in the current international context. Moreover, this new generation warfare imposes a specific analysis at the level of international scientific community also due to the fact that it does not present a pre-established "pattern", but both state and non-state actors oscillate using it, up to the necessary period it takes to win a dispute by applying all the defining measures and elements of hybrid warfare.

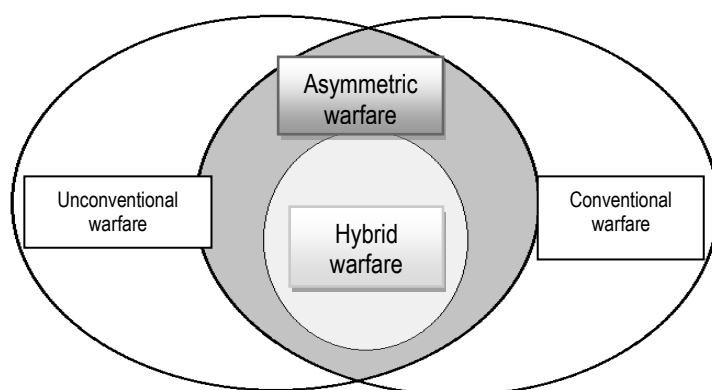


Figure 1. The place of new generation warfare among major conflicts

⁴ Buța Viorel, Valentin Vasile, *Studiu privind metamorfozele războiului hibrid*, București 2016.



From the studies made until now by the international academic community on hybrid warfare, we may pick a few defining elements that actually lead to generating and perpetrating this new “trend” which is gaining more and more ground in conducting military actions, especially within the so called "frozen conflicts" spread everywhere on the map of international relations. These elements, which are common can be found equally within conventional, unconventional and asymmetric warfare, in a cumulated manner lead to what the international community assimilates as "new generation warfare" or "hybrid warfare"⁵:

- Infiltration – in the force institutions of the enemy, politically, economically, and in the armed forces of a state. The latter represents a vulnerable element and once destabilized and won over by the enemy it makes hybrid warfare relatively fast to win, without the use of armed force and with a low resource consumption.

- Undermining – economy and commerce by preventing, through various methods, the normal conduct of economic activities and thus causing it serious damage. In addition, by the violent actions taken by groups of people with the purpose of weakening state power, the ultimate stage is the total shut-down of a system which may counter a significant part of new generation warfare.

- Subversion – an element occurring in the conduct of hybrid warfare in close connection with undermining actions, its peculiarity being conducting fake actions for disorganizing the enemy, with major implications upon the leadership of the state, armed forces, and other institutions that make up the rule of law.

- Disinformation – launching fake information, apparently credible and at the same time blaming institutions, influential people and decision-makers in key positions, with the purpose of facilitating obtaining the necessary results for winning hybrid warfare.

- Decreasing morale – in very close connection to disinformation, having as main goal determining the enemy to give up and finally accepting the propositions of the enemy in order to reduce collateral damage.

- Resources – they are another particular feature of this type of new generation warfare. The resources used in waging such a war can be quite

⁵ Florina Mihaela Nicolescu, *op. cit.*



high and time-consuming at a first comparative analysis with the living standard and the fewer and fewer resources available after each decade that closes chapters of world history. Yet, when comparing it with the other types of wars presented in Figure 1 and at the same time putting in balance the loss suffered through the years in the conflicts that affected the world, hybrid warfare remains an alternative that is more and more used in international conflicts.

- Globalization – a term that is similar to other concepts which can be found in the vocabulary of political sciences such as democracy and power, still remains a controversial term, difficult to be included in a certain precise definition, universally acceptable within international academic environment. This has allowed the multiplication of fiscal paradises, companies, and cover banks, which led to a major misbalance, on a global scale, between the poor and the rich countries, making the latter even poorer in order to make the former obviously richer, as well as in order to bring additional capital to non-state actors with the purpose of intervening in certain hot spots on the globe.

- Internet – together with globalization, it represents the main elements that make hybrid warfare acquire distinct features function of the nature of military actions conducted in a certain area on Earth. The aggressive propaganda, incitement to violent actions, recruiting personnel that is specialized in certain domains connected to military actions, radicalization through indoctrination, financing actions that are covering the real interests, the detailed planning of actions meant to contribute to accomplishing the desired goals, social-media by conducting vast operations of mass influencing with the help of influencers make the Internet a defining element for hybrid warfare and at the same time an element worthy of being monitored permanently due to the fact that it is in a continuous technological expansion. Moreover, hybrid warfare thus suffers mutations, becoming very difficult to be categorized in a certain pattern by the academic community.

Hybrid warfare has specific elements such as the presence of individuals dressed in military uniforms without insignia that might indicate their belonging to a certain army; promoting and propaganda of fake information and ideas with the aim of destabilizing a region, using insurgent tactics such as kidnappings, drug trafficking, torture with the aim of



destabilizing and frightening the population, the aggressive campaign of cyber-crime at the same time with a lack of a strong cyber-security strategy. These are all continental practices specific to a hybrid war conducted from the land towards the sea and were all of them included in a vast land operation; however, this is about to change due to the more and more eloquent involvement of navy powers in the conflict areas.

Although this new generation warfare was brought into public attention due to the annexation of Crimean Peninsula by the Russian Federation in 2014, as it was shown at the beginning of the present paper, the international academic environment dealt very scarcely with the maritime component which played a key role in the war waged in the most strategic point of the Black Sea by the Russian Federation, as well as the implications upon this component upon the annexation of Crimea to the homeland.

Conducted on a certain territory and re-launched together with the invasion of Ukraine by the Russian Federation, hybrid warfare is rather associated with a land warfare, having the land component directly in charge with its execution. Actually, this is only partly true, as the naval component is also present in most stages of a hybrid war, having implications and missions specific to the new generation warfare.

Furthermore, the involvement of naval power in a hybrid war is an element that needs to be taken into consideration when studying the new generation warfare, which gives rise to questions such as: which are the peculiar aspects of navy missions in a hybrid war? What kinds of training are necessary for a naval power to be able to face hybrid threats and at the same time to be able to execute missions within a new generation war? Should there be new naval structures specialized in fighting maritime hybrid threats? How should the naval power of a state be adapted in order to be able to face the new types of threats? Which could be the consequences of hybrid actions to what the Navy stands for nowadays? All these questions are also derived from the fact that the latest actions specific to hybrid warfare recognized at international level also happened 200 nautical miles from Romania's territorial waters.

The Navy component of a state can execute a vast range of missions, being attributed elements such as defending and promoting a state's interests, independently or together with other forces given the membership



to North-Atlantic Alliance, the EU, as well as other regional and international organizations, through participation and conducting operations in the area of responsibility both on the sea and from the sea towards the land, in order to preserve the territorial integrity and maintaining freedom of navigation on the maritime communication ways. Moreover, the naval power of a state contributes to ensuring regional stability, collective defense in the alliance and military coalition systems, by participating in actions for peacekeeping or peace making⁶.

As for the use of a state's naval power in conducting actions in a hybrid war, James G. Stavridis, retired admiral, US Navy and former commander of Supreme Headquarters Allied Powers Europe (SHAPE), stated that there are four major advantages of using the naval component in hybrid warfare as follows:

- It allows a state or non-state actor, by means of the naval component, to undertake actions of intimidation, deterrence, neutralization and suppression of the enemy's capabilities behind deception actions regarding the purpose and objectives of real actions. The naval actions of intimidation and deterrence are largely encountered on the world's seas and oceans, especially in the interest zones for the great maritime powers of the world such as the East of Mediterranean Sea, Black Sea, North Sea, Baltic Sea, Persian Gulf, Aden Gulf etc. The main characteristic feature of these types of actions is represented by the freedom of navigation on the planetary ocean, which makes the naval presence in the international waters of a certain area of interest not draw criticism and sanctions from the international community;

- The use of maritime component in hybrid warfare involves surprising the enemy who is thus rendered unable to anticipate the presence, landing, insertion and troop movements that are about to happen in the conflict zone. Moreover, it cannot anticipate fire or air support offered on maritime platforms to the troops conducting actions from sea towards land;

- The tactics and techniques used by the maritime component in hybrid warfare can offer security and accuracy in executing the missions. They may impose the pace, control and follow the chronological unfolding of the events initially planned. The layout of the flag ship or platform which

⁶ ***, *Constituția României*, Editura Rosetti Internațional, București, 2015, p. 47.



offers command and control over hybrid actions conducted from the sea towards the land at a safety distance and equipped with sensors and armament systems which may counter an entire spectrum of threats in different environments represent another element specific to the hybrid warfare involving naval forces;

- The use of small, well-equipped, ships which might counter different types of threats presupposes smaller costs in comparison with the use of classical maritime platforms. Conducting this type of warfare essentially presupposes smaller costs in comparison to other types of warfare waged in history, the main element that needs to be taken into account being adapting the existing resources in order to be able to face the new kinds of threats which are increasingly present in international relations⁷.

In this regard, the role of Navy in countering land hybrid actions should be reconsidered by using their defining elements: sea fleet, Danube flotilla, combat divers, special operation forces, marines, naval air assets etc. All these capabilities meant to counter and fight hybrid sea threats can be used along coast lines as well as in the interior waters from the seashore in what could be called the hybrid warfare from sea to land, being an important component of the new generation warfare.

The use of the naval component in a hybrid war may take on unexpected features such as the use of small ships without distinct inscriptions in the seashore area for logistic actions, surveillance, forward observation point, command and control or enemy intimidation and deterrence. Nevertheless, the main elements of a new-generation warfare are also going towards the naval domain, the involvement of maritime component being more and more visible and significant in the conduct of hybrid actions, especially those from sea to land.

In conclusion, the international community should be aware of the existence of this type of warfare, a 4th generation warfare, according to some researchers, to try to give it a definition as close to reality as possible, and study its tendencies of development in the sense of establishing a set of measures that need to be taken in order to ensure its early countering.

⁷ James G. Stavridis, *Maritime hybride warfare is coming*, accessed on 25.09.2019, at <https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming>.



At the same time, another direction of research should be the impact that the naval component might have in a hybrid war, as well as the manner of adjusting the naval forces to the new types of threats specific to the new generation warfare.

Last but not least, the membership to organizations of collective defense, such as North Atlantic Treaty Organization presupposes creating and adopting a strategy regarding hybrid warfare in order to act independently, unitarily or jointly in case of actions assimilated to new generation warfare. This comes naturally also due to the fact that so far the North Atlantic Alliance has not taken a firm stand regarding hybrid warfare by recognizing it as a permanent threat to the borders of the Alliance.

By promulgating Allied Joint Doctrine AJP-01(D), by NATO Standardizing Agency on 21st December 2010, the North-Atlantic Treaty Organization admitted a possible use of hybrid threats by the enemies interested in exploiting the vulnerabilities of the Alliance, who are pursuing their objectives by applying long-term strategies, focused not on obtaining the victory but rather on avoiding defeat⁸.

Hybrid warfare uses the Chinese drop, it has time on its side and its peak will most of the time a place of no return, when the implementation of countering measures and the algorithm "discovered" by researchers are going to come too late and will result in an asymmetric or unconventional conflict.

Bibliography

1. *** *Constituția României*, Editura Rosetti Internațional, București, 2015.
2. *** European Network and Information Security Agency (ENISA). *Analysis of Cyber Security Aspects in the Maritime Sector* (Heraklion, Greece: European Network and Information Security Agency (ENISA).
3. *** "Maritime Cyber Attack – A Clear and Present Danger".

⁸ Buța Viorel, Valentin Vasile, *Considerații privind perspectiva NATO asupra războiului hibrid*, Revista de Științe Militare editată de către Academia Oamenilor de Știință din România, issue 1 of 2015.



4. *** Hybrid warfare: NATO'S new strategic challenge?, draft generak report, Julio MIRANDA CALHA (Portugal), General Rapporteur.
Academia Română,
5. Institutul de lingvistică "Iorgu Iordan – Al. Rosetti" *Dicționarul explicativ al limbii române*, Editura Univers Enciclopedic, București, 2016.
6. Buța, Viorel *Tendințe actuale în domeniul științe militare*, Revista Academiei de Științe ale Securității Naționale, numărul 1 din 2016.
7. Buța, Viorel; Valentin, Vasile *Considerații privind perspectiva NATO asupra războiului hibrid*, Revista de Științe Militare editată de către Academia Oamenilor de Știință din România, numărul 1 din 2015.
8. Buța, Viorel; Valentin, Vasile *Răzbiul de tip nou: perspectiva Rusă*, Gândirea Militară Românească, numărul 2 din 2015.
9. Buța, Viorel; Valentin, Vasile *Perspectivile asupra evoluției și influenței conceptului de război hibrid (I)*, Gândirea Militară Românească, numărul 3 din 2015.
10. Buța, Viorel; Valentin, Vasile *Perspectivile asupra evoluției și influenței conceptului de război hibrid (I)*, Gândirea Militară Românească, numărul 4 din 2015.
11. Buța, Viorel; Valentin, Vasile *Studiu privind metamorfozele războiului hibrid*, București 2016.
12. Colectiv F.N.-1, Doctrina Forțelor Navale.
13. Florina Mihaela, Nicolescu *Războiul hibrid. Perspectiva conceptuală rusă*, pe <https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa>.
14. James G., Stavridis *Maritime hybride warfare is coming*, pe <https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming>.
15. Mattis, J. N.; Hoffman, F. *Future Warfare: The Rise of Hybrid Wars*, U.S. Naval Institute, Proceedings Magazine.
16. Frunzeti, Teodor; Bușe, Dorel *Relații internaționale*, Editura Universității Naționale de Apărare "Carol I", București, 2011.



APPROACHING MILITARY ART FROM A HERMENEUTICAL PERSPECTIVE

Colonel (r.) Professor Ion MITULEȚU, PhD

Tenured member of the Academy of National Security Sciences,

E-mail: mituletuion@yahoo.com

Abstract: *Approaching military art from a hermeneutical perspective aims at presenting certain points of view regarding the use of normative-logical instruments for interpreting, understanding and deciphering the sense of concepts it covers.*

In this context, the scientific language used for expressing the concepts specific to military art has to respect the rules of hermeneutical logics, materialized in the general picture that comprises initial knowledge, interpretation, and understanding; its outcome is obtaining deep knowledge (added-value in knowledge).

The relations established among the components of military art – strategy, operational and tactical art – are based on integrating, inter-connecting, correlating, synchronizing and coordinating objectives, command and control structures, forces, high-quality combat technique, information technologies, protection and support equipment to the purpose of obtaining a synergic effect within the whole range of military operations.

The profound mutations in the multi-dimensional operational environment, analyzed from a hermeneutical perspective, determines the following types of strategies: conventional, unconventional, alternative, mixed.

Keywords: *hermeneutics, military art, strategy, operational art, tactics, extended operational environment.*

Hermeneutics between interpretation and understanding

Hermeneutics is the discipline that uses the methods of interpretation and understanding of concepts circumscribed to a branch of science or some of its domains, to the purpose of identifying the sense and essence of the phenomena determining it, as well as their evolutions in time and space¹.

¹ www.diacronia.ro/ro/indexing/details/A22638/pdf (“Textul” ca propunere de “lume” între explicație și înțelegere), accessed on 14.10.2019.



In this context, the key concepts of hermeneutics – interpretation and understanding – have the end state of developing knowledge and, by doing that, formulate hypotheses which might lead to deciphering the premises of evolution of the concepts specific to the respective domain.

Hermeneutics is an art instituting clear rules of interpretation (having the character of norm) and reflection upon the interpreted phenomenon².

Thus, the normative-logic character of hermeneutics, materialized in instituting clear rules for interpreting concepts, notions, syntagms, and paradigms in the respective domain, ensures prospective reflection upon the manner of deciphering their meanings and future trends of evolution.

As a theory of interpretation rules, hermeneutics is a stage of logics which, through induction and deduction, discovers the meanings of concepts and validates the succession of phases in which they are going to evolve.

Thus, hermeneutics offers the methodological frame of analysis and interpretation of concepts in order to decipher the meanings and senses specific to decoding the messages that may have different meanings; therefore, it needs rigorousness in formulating judgements regarding redefining, re-evaluating, or re-interpreting them.

In this regard, an interpretation cycle is initiated which starts from an initial point which targets the stage of knowledge in the respective field, it goes further through successive logical operations (logics of induction and deduction) where the senses of phenomena and their evolutionary trends are interpreted and understood, finally reaching the end state which expresses superior knowledge, that is, added value in knowledge³.

From the hermeneutical point of view, understanding means an act of creation, namely putting forth personal and original points of view regarding the intention of redefining the concepts subject to analysis, reinterpreting and arranging them in logical order within the respective domain.

That is why we can say that hermeneutics uses specific instruments to critical spirit, expressed through the capacity of interpretation of concepts and phenomena, using logical and coherent demonstration, in order to be

² <https://ro.scrib.com/document/About-Hermeneutics>, accessed on 14.10.2019.

³ www.autorii.com/scriitori/sinteze-literare/precizări-metodologice-hermeneutice-și-poetica.php, accessed on 14.10.2019.



correctly understood and adequately deciphered in point of meanings and evolutionary trends.

Taking into consideration the fact that hermeneutics is a rational act, it uses "strategies of interpretation" in order to validate, understand the meaning and evolutionary trends of specific concepts and the "hermeneutical reflection" whose character is prospective, as it oriented towards the future.

Thus, the general pattern of the hermeneutics concept implies the use of the following algorithm: initial knowledge, interpretation, understanding (sense, evolution, action), enriched knowledge (added value in knowledge).

Taking into consideration the theoretical elements presented above we may naturally answer the question: *Can military art be approached from a hermeneutical point of view?*

The answer we may give aims at revealing the necessity of approaching military art, as the complexity and diversity of concepts, syntagms, notions and paradigms circumscribed to this complex domain, impose identifying some logical and coherent modalities of interpreting, deciphering, and understanding their meanings in order to eliminate ambiguities, confusions, and exaggerations in communication and action.

Hermeneutics, through the methods and instruments used, helps us become prepared to enter the complex maze of military art in order to discover, interpret and understand their meaning. That is why we consider that this pragmatic approach aims at creating a theoretical-methodological frame meant to provide not only the capacity of reaction and adaptation, but also the capacity of anticipation and pro-active action in preparing and conducting the military operation.

From this point of view, our aim is to demonstrate the importance of hermeneutics in approaching military art by developing the following issues: the scientific language used in expressing concepts; the relations established among the components of military art; the typology of strategies resulting from the hermeneutical perspective.

The scientific terminology used in expressing concepts

Although hermeneutics has a universal character, being possible to apply it in all scientific branches, we should state that the terminology used should be adequate, adapted and coherent so as to understand and correctly



use concepts, syntagms, notions and paradigms defining military science, respectively, military art, as its main components.

In this respect, the literature in the field considers hermeneutics a general theory of language, which turns unclear and ambiguous concepts in clear and coherent expressions⁴.

That is why, we consider it useful to apply a standardized scientific terminology in defining, interpreting, and understanding the concepts specific to the military domain, both generally speaking and at the particular level of military art.

At the same time, we consider that using a standardized terminology positively influences the understanding of concepts circumscribed to the military domain (military art) and increases the efficiency of communication at the level of national and multinational military structures.

Thus, we may say that the standardization of the terminology used in the national and NATO commands and military structures becomes an essential condition of understanding operation planning, communicating orders and assigning missions.

Furthermore, the use of hermeneutical methods and instruments helps both the command and the execution staff to acquire a pragmatic interpretation of specific concepts, to correctly understand their meaning, to decipher their tendencies, constituting the convergence point which makes it possible to efficiently communicate at military-strategic, operational, and tactical levels.

At the same time, the standardization of military terminology has to be accompanied by scientific rigor, so that, the meanings of concepts, syntagms, and notions used by military personnel (commands and military structures) in the planning, preparation, execution, and evaluation of the operation in national and multinational context (Alliance, coalition) might have the same meaning, not to create ambiguities or confusion in communication and transmitting messages (orders).

That is why we suggest that the leadership personnel at military-strategic, operational, and tactical levels, as well as the teachers in the system of military education use the methods specific to hermeneutics (normative-logical, deduction and logical inference, etc.) in order to

⁴ <https://ro.scrib.com/document/About-Hermeneutics>, accessed on 14.10.2019.



rigorously interpret the specific concepts so as to lead to their correct understanding as well as their tendencies in evolution.

In this regard, we can apply the general pattern of hermeneutics that leaves from the initial knowledge of concepts, followed by the process of interpretation and understanding their meanings, the nature of relations established among components and deciphering their future trends, so as, in the end, to have as outcome the added value in the acknowledgement of the respective phenomenon.

Another result is that introducing and approaching new components in the field aim at defining, interpreting and understanding them in relation to current terms, applying the general pattern of hermeneutics presented above.

Approaching these theoretical elements regarding the necessity of using hermeneutical methods that might ensure defining, interpreting and correctly understanding the concepts specific to military art needs to become a permanent concern of military personnel in order to develop a culture in the field which could result in the rise of a new generation of military leaders⁵.

Without promoting a culture in the field that might offer military leaders the possibility of rigorously interpreting and correctly understanding concepts, notions, and syntagms specific to military art, there will be ambiguities and lack of precision in the planning, communicating, and transmitting orders, respectively, missions.

Culture in the military domain has the following features: wisdom; active adaptation; realism; experience⁶.

Wisdom presupposes the cognitive capacity of the individual to correctly interpret the concepts, notions or syntagms to be rigorously understood and applied in the planning, preparation, and execution of military operations.

Active adaptation is the process through the individual, based on the use of critical (hermeneutical) instruments is able to timely detect the

⁵ *Strategia Militară a României*, București, 2016, p.10.

⁶ Mircea Malița, *Cumințenia Pământului: Strategii de supraviețuire în istoria poporului român*, Ed. A 2-a, rev., București, Ed. Compania, 2012, p.21.



changes occurring within the concepts and phenomena subject to analysis and decipher the new meanings in understanding and applying them.

Realism refers to the rigor with which the specific syntagms, concepts and notions are standardized in order to be interpreted and understood coherently and in a unitary manner, without distortions, confusions, or ambiguities.

Experience comes from the profound studies of the military domains, from the culture in the field that is acquired and developed in time, thus ensuring the correct interpretation and understanding of concepts, notions and syntagms used in planning, preparing, executing and evaluating operations, in a national and multinational context.

In the pages below we are going to use the general pattern of hermeneutics in order to define, interpret and understand the meanings and evolutionary trends of the levels of military art: strategic (military-strategic); operational; tactical.

Step 1 – Initial acknowledgement of the concept

The strategic (military-strategic) level has to do with a nation that sets objectives of national security for itself and allocates resources of any kind, including the military kind, in order to accomplish them in campaigns or major joint operations⁷.

Step 2 – Interpretation of the concept

The strategic (military-strategic) level is directed by the political leadership, it has a strategic command and control structure available, it uses national power instruments (military and non-military), it accomplishes strategic goals for reaching the political end state, it allocates the necessary forces and means for conducting the major joint campaign / operation, it plans strategic operation, it transmits the military-strategic plan (strategic execution order).

Step 3 – Understanding the concept

The sense in which the strategic (military-strategic) level should be understood has to do with the following elements: it has as objects of study warfare (conflict) and armed fight; war (conflict) continues to be an instrument of politics; it has a strategic (national or multinational) command

⁷ SMG-3, *Manualul de planificare a operațiilor*, București, 2016, p.192.



that analyses PMESII⁸ systems; it uses military and non-military power instruments; it establishes the level of effects, thus ensuring the accomplishment of strategic goals and achieving the political end-state; it involves military and non-military force structures for a joint, inter-institutional response in hostile operation environments⁹; it combines soft and hard power instruments; it uses high technologies and modern information systems that produce mutations in the physiognomy of war (conflict).

Step 4 – Evolutionary trends of the concept (added-value in knowledge)

We notice that at strategic (military-strategic) level, it becomes a true means of deterrence combining several instruments of power. At the same time, although conflicts maintain their violent and destructive character, we notice that their center of gravity is moved towards their cognitive and information dimensions, thus giving birth to new forms of military operations.

Moreover, the distinction peace, crisis, war (conflict) becomes faded, actions being diversified in order to counter all the potential risks and threats in the operational environment.

Step 1 – Initial acknowledgement of the concept

The operational level is the manner in which battles or operations are planned, executed and supported in order to accomplish the strategic goals established for the joint operations area¹⁰.

Step 2 – Interpreting the concept

The operational level is directed by the strategic (military-strategic) level; it has a joint command and control structure; it uses the joint forces and means allocated (land, air, sea); it accomplishes the strategic objectives established and the political end-state. At the same time, it plans and executes the joint operation plan/order, established by the military-strategic

⁸ Political, military, economic, social, infrastructure, and information systems existing in the area of engagement and which can create unacceptable conditions for the national or NATO (EU) interests.

⁹ *Strategia Militară a României*, București, 2016, p.15.

¹⁰ SMG-3, *Manualul de planificare a operațiilor*, București, 2016, p.192.



command. It elaborates and transmits the operation plan / order towards the subordinated structures.

Step 3 – Understanding the concept

These sense in which the operational level covers the following elements: it has a joint (national or multinational command) that analyses PMESII systems; it uses joint force; it establishes the level of effects, thus ensuring the accomplishment of strategic objectives and the political end-state; it leads the available forces and means in the joint strategic operations, except for the strategic reserve and the special operations forces, even if they are in their area of responsibility; it uses advanced technologies and information systems that generate new types of joint operation conducted in an extended operational level.

Step 4 – Evolutionary trends of the concept (added value in knowledge)

At operational level we witness the emergence of new forms of military operations, following the integration and inter-connecting of high technologies and information systems, as well as diversification of risks and threats at operational level.

In this regard, we notice the existence of a wide range of joint military operations, highly technologized and super-fast which are network-based, effect-based, irregular (asymmetric), psychological, information, cyber etc.

Step 1- Initial knowledge of the concept

The tactical level is the manner in which strikes and fights are planned and executed in order to accomplish the military objectives of tactical units and major units¹¹.

Step 2 – Interpretation of the concept

The tactical level is directed by the operational level, it has land, air, and naval command and control structures; it uses subordinated forces and means; it accomplishes the tactical purposes established for achieving operational goals. Also, it plans and executes actions in the operation areas established at operational level. It elaborates and transmits the operation order / plan to the subordinated structures.

Step 3 – Understanding the concept

¹¹ SMG-3, *Manualul de planificare a operațiilor*, București, 2016, p.192.



The meaning of the tactical level has to do with the following elements: it has tactical commands at the level of land, air, and naval forces, as well as units and major units; it uses the force structures available; it establishes the level of effects, thus ensuring the accomplishment of operational objectives; it leads the forces and means available in the area of operations established; it uses advanced technologies and information systems that generate new forms and procedures of operation (battle).

Step 4 – Evolutionary trends of the concept (added value in knowledge)

At tactical level we notice the emergence of new forms and procedures of fighting, following the inter-connecting, on the one hand, of high technologies and information systems and, on the other hand, the diversification of risks and threats in the operational environment.

In this regard, we notice the existence of a large range of combat procedures, executed by regular (conventional), irregular (asymmetric), proxy (through interposed troops), non-kinetic or mixed forces.

Relations established between the components of military art

Hermeneutics offers us not only a model based on information and research regarding the concepts and phenomena ensuring the expression of own view points, but also the methodological frame in which relations can be analyzed among the components of military domain.

In this regard, we thought it would be interesting to outline the nature of relations established among the components of military art in order to have a comprehensive, unitary approach of the conflict conducted in the multidimensional operational environment.

The threefold concept strategy, operational art, and tactics can be regarded as a system of systems which integrate, inter-connect, relate, correlate, synchronize, and coordinate purposes, objectives, effects, command and control structures, forces, high combat technique, information technology, protection and support equipment.

Thus, we may state that the relations existing among the components of military art need to be known, interpreted, and understood in order to bring benefits to obtaining information superiority, rendering the decision more efficient, and increasing the effects of the actions executed in the whole range of military operations.



In this context, we consider that making use of adequate capabilities which are dimensioned and configured according to the nature of the threat aims exactly at emphasizing the manner of inter-relating among components, structures, and systems that might ensure the objectives and desired end state.

That is why, it becomes increasingly important to have a comprehensive approach of the conflict in which power instruments (of the parties) involved act in a coordinated and coherent manner in order to manage the situation created.

A first element of inter-connection regards cooperative planning (joined, parallel) at strategic, operative, and tactical levels in order to reduce the time necessary for decision-making, elaborating the operation plan / order and transmitting the missions in order to accomplish the objectives established¹².

When we refer to the complex command and control systems of C4ISR type (command, control, communications, computers, intelligence, surveillance, reconnaissance), respectively C4ISTAR (command, control, communications, computers, intelligence, surveillance, target acquisition, reconnaissance), they integrate, interconnect, relate and synchronize sensors, decision-makers, and land, air, naval battle platforms, the conflict thus acquiring new characteristics materialized in network-based operations (information operations), respectively, effect-based operations (selective approach regarding the level of destruction).

Regarding the forces and means engaged in conflict, the degree of interconnection is aimed at preparing them through repetitions, coordination of the operation on stages and missions. This is how we obtain the synergic effect in the field of information, decision, and action, oriented through cooperation, synchronization, and mutual support.

Regarding the inter-connection during planning, preparation, and execution of military operations within NATO, we consider that it is mandatory to have compatibility and inter-operability, both within strategic, operational, and tactical levels and at the levels of forces in order to ensure the adequate accomplishment of missions.

¹² SMG-3, *Manualul de planificare a operațiilor*, București, 2016, pp.13-14.



The conclusion of this approach is that the connections established among the components of military art happen from upwards downwards, from strategic defense that directs the operational level and, in turn, this directs the tactical one, and the results (the accomplishment of objectives) is performed from downward upwards, so as the accomplishment of missions at tactical level may ensure the accomplishment of operational goals, strategic objectives, and final political end-state.

Typology of strategies resulting from the hermeneutical perspective

The complexity of the operational environment, the diversity and dynamics of risks and threats, the multitude of state and non-state actors, they all determine essential changes in the features of the military conflict and generate new forms of military operations.

That is why we consider that it is imperative to reassess and reinterpret current strategies in order for them to reflect the new circumstances created in the multidimensional operational environment.

Taking into consideration these elements, hermeneutics offers us the logical-normative framework of interpretation and understanding of the essence of strategies that might answer to the tendencies in evolution of military art.

In this context, we can say that there are the following types of strategies: conventional, unconventional, alternative, mixed.

Conventional strategies are meant to use the military instrument, materialized in armed force to the purpose of accomplishing strategic objectives and reaching the final end-state established by the political decision-maker.

Conventional strategies have as a center of gravity armed fight, characterized by violence and destruction, in comparison with the purposes of the campaign or major military operations.

In this sense, the conventional approach of the conflict includes planning, preparing, and executing the strategic joint operation, which may be offensive or defensive.

The strategic joint operation has a national or multinational character; it takes place in a theater of operations; it is led by a strategic command; it comprises military forces (land, air, navy, special operations,



communications and IT, CBRN, logistic support) and non-military; it accomplishes the strategic objectives fulfilled in order to accomplish the political end-state.

Integrating and inter-connecting advanced technologies determine clear changes in the features of conventional conflict. In this regard, changes are made within the command and control systems that integrate technologies and IT equipment at the force component level by assimilating state of the art combat technique that provides mobility and efficiency in the rapid neutralization of enemy targets.

These high technological elements, integrated to force structures, determine the following: the highly technologized and rapid strategic joint operation; smart defense; network-based operation; effect-based operation, etc.

If in the past conventional operations were conducted in almost similar conditions, within which there was a power balance, the effort made in the technological field aimed exactly breaking up this balance and creating a certain lack of symmetry, an operational lack of proportions among the enemies that might lead to the victory of those endowed with high systems, technologies, equipment.

The technological gap between enemies reduced the conflict area at local and regional level and introduced the concept of conventional deterrence which NATO is particularly keen on.

These are the reasons why we consider that the states that are going to have and integrate high technology in the armed forces (information, artificial intelligence, armaments, and adequate ammunition, etc.) are going to create that operational gap that will result in their deterrence of potential enemies, not only at cognitive, but also at moral level too.

Non-conventional strategies have as a main vector the nuclear weapon. The existence of nuclear capabilities within the endowment of some states or at NATO level has generated the strategy of dissuasion, respectively, deterrence strategy.

Thus, *deterrence strategy* has as a purpose persuading the enemy not to act because of the consequences that the use of nuclear weapons might inculcate.



The deterrence effect is created by the destructive effects of the nuclear weapon, being put into theoretical terms under the name of resilience deterrence or the deterrence through strength¹³.

The nuclear deterrence strategy usually aims at obtaining political advantages, the states that have nuclear vectors being privileged in international relations.

NATO has expanded the area of deterrence and defense through an adequate, proportional and credible combination of nuclear capabilities and the conventional defense capabilities against ballistic missiles.

Thus, supporting nuclear deterrence is the basic element of collective defense, the strategic nuclear forces of the Alliance representing the supreme guarantee of the security of member states¹⁴.

The aim of NATO nuclear capabilities is to keep peace, prevent constraints, and deter potential enemies¹⁵.

Russian Federation supports the strategy of nuclear dissuasion and deterrence as a main vector of defense against the Alliance.

Nuclear proliferation is a major concern for regional and global security and that is why the efforts of international states and organizations need to be directed towards firm measures of counter-proliferation and control of the armaments and vectors of this type.

Alternative strategies are mainly based on asymmetry as a reaction of mostly non-state actors to compensate through atypical means and procedures, the technological, information, and decisional superiority of the enemy.

The category of asymmetric operations includes insurgence, guerilla, terrorism, and organized crime.

Alternative strategies aim at irregular operations among which counter-insurgence, counter-guerilla, counter-terrorism and counter-organized crime activities¹⁶.

¹³ Herve Coutau-Begarie, *Breviar de strategie*, Ed. Sitech, Craiova, 2002, pp.52-53.

¹⁴ *Final NATO Statement, Bruseles Summit*, 11-12 July 2018.

¹⁵ *Ibidem*.

¹⁶ AJP-01, *Allied Joint Doctrine*, Edition E, Version 1, February, 2017, 2-21, 2-22, 2-23.



These types of operations go beyond the joint level of the conflict, having an integrating character and being conducted in an inter-institutional framework.

Mixed strategies have to do with operations combining several types of actions among which conventional, unconventional, asymmetric, cyber, psychological, information, media, economic, political, etc.

Mixed strategies include hybrid conflicts and variable geometry conflicts.

The hybrid conflict comprises a whole range of non-kinetic operations (information, cyber, psychological, media), kinetic (missile systems, air and navy platforms), irregular (proxy, through interposed parties) and unconventional (special operation forces under the disguise of regular people) conducted in an area of strategic interest in order to morally and cognitively affect the potential enemy and accomplish political objectives.

The conflict with variable geometry comprises the operations that change and adjust function of the operational situation created; it is possible to start off with a civil warfare within a failed state, to continue with irregular actions (insurgence, counter-insurgence, guerilla, counter-guerilla, terrorism, counter-terrorism), conventional actions and procedures (air attacks), unconventional (special operations), non-kinetic and proxy, supported by the sponsor-states.

Taking into account the multitude of state and non-state actors involved in the conflict with variable geometry, strategic and political goals are different and heterogeneous, being prone to harmonization only through political and diplomatic actions in order to create a state of stability in the affected area.

Conclusions

Given the fact that military art has broadened its content and the military operations conducted at strategic, operational, and tactical levels have modified their features, acquiring new characteristics and dimensions, it becomes mandatory to use the methods of hermeneutical logic in order to give coherence and rigor to the interpretation and understanding of the essence and meaning, as well as to deciphering the evolutionary trends of the specific concepts.



The concepts specific to military art subject to hermeneutical interpretation can be systematized, standardized, applied in a unitary, unequivocal manner in the planning process, communication process and conveying of orders, at national level and in a multinational context.

Understanding the essence and tendencies in evolution of the concepts circumscribed to military art can be capitalized in elaborating realistic strategies, adaptable and credible in relation to the dynamics of security environment, the diversity of actors involved and the potential threats.

These elements can be known and understood only by developing a solid education and by training a new generation of military leaders capable of identifying the changes produced in the security environment and elaborate the adequate and credible response options at strategic level.

In order to formulate and assert judgements, hermeneutics is also a "discipline of thinking", that makes up the interference point that gives meaning to the interpretation and understanding of military concepts.

Finally, even if we accept that there is a "conflict of interpretations" between Hermes (the Greek god of communication and interpretations) and Ares (the Greek god of war), the dispute may be settled through rigorousness, coherence and credibility in the effort of acknowledging, interpreting, and understanding the complexity of the military phenomenon.

Bibliography

1. * * * *Strategia Militară a României*, București, 2016.
2. * * * *SMG-3, Manualul de planificare a operațiilor*, București, 2016.
3. * * * *Declarația Finală a Summitului NATO*, 11-12 iulie 2018.
4. * * * *AJP-01, Allied Joint Doctrine*, Edition E, Version 1, February, 2017, 2-21, 2-22, 2-23.
5. Herve, Coutau-Begarie *Breviar de strategie*, Editura Sitech, Craiova, 2002.



6. Mircea, Malița *Cumințenia Pământului: Strategii de supraviețuire în istoria poporului român*, Ed. A 2-a, rev., București, Editura Compania, 2012.
7. * * * www.diacronia.ro/ro/indexing/details/A22638/pdf
(“Textul” ca propunere de “lume” între explicație și înțelegere).
8. * * * <https://ro.scrib.com/document/About-Hermeneutics>.
9. * * * www.autorii.com/scriitori/sinteze-literare/precizari-metodologice-hemeneutice-si-poetica.php.



IS IT TIME TO LOSE THE MDMP WITHIN THE ROMANIAN ARMY?

Brigadier General (ret.) Professor Viorel BUȚA, PhD
Tenured member of Academy of National Security Sciences,
Tenured member of the Academy of Romanian Scientists,
E-mail: vbuta49@yahoo.com

Lieutenant Colonel Irinel APOSTOLESCU, PhD student
Ministry of National Defense,
E-mail: i_apostolescu@yahoo.com

***Abstract:** The military decision-making process existing in the Romanian Army is permanently criticized for being highly time-consuming, unrealistic, dogmatic and unimaginative. Also, there is a mismatch between the stages of the Operational Planning Process and the military decision-making process. The currently existing planning manuals comprise long and detailed information about the planning process carried out at strategic or operational level and adjacent to the tactical level. The purpose of this material is to demonstrate that the MDMP (Military Decision Making Process), as it is implemented, is not an optimal process and, at the same time, to propose an alternative MDMP model that not only fits the Romanian reality and way of thinking better, but also offers a better connection with the doctrinal stages of the operational planning process.*

***Keywords:** decision, planning, process, military organization.*

1. Short overview of doctrine provisions

The OPP – Operational Planning Process – and the recent operations of NATO – North Atlantic Treaty Organization – demonstrate how the international community needs to collaborate in a more efficient manner and adopt a comprehensive approach with respect to keeping international peace and security.

Such an approach necessitates the cooperation of all the major actors involved, including IO – international organizations – and NGOs – Non-governmental organizations, as well as relevant agencies and organizations in the area of joint operations. An efficient implementation of any action



plan necessitates the concentration of efforts, increasing responsibility and motivating all actors.

In order to maximize the ability to operate in an exhaustive manner, the Alliance wishes to improve the crisis response procedures and capabilities and increase cooperation at all levels with all external actors, including those involved in stabilization and reconstruction missions. Starting with the operation level, the commander and his staff needs to take into account, maybe just as much as conducting military actions, the interaction with various entities and organizations and the impact of military actions upon their activity.

NATO policy states that, at operation level, the priority should be cooperation with the other international actors involved in the planning process of an operation in which it is necessary to interact with these entities. At the level of theater of operations, the commander has to be mandated to also involve local authorities in execution.

Stages of planning process – operation level. The operation planning process – operational level, comprises the necessary steps so that the joint force commander (JFC) and his staff may make the operation plan at operational level. The stages also include the continuous assessment of the operation in order to be able to revise or amend the plan, when it is necessary.

The steps of operational planning at operational level are the following:

Step 1 – Initiating planning.

Step 2 – Mission analysis.

Step 3 – Elaborating the courses of action (COA – Course of Action).

Step 4 – Analyzing COA.

Step 5 – Comparing and validating COA.

Step 6 – Commander’s decision regarding the choice of COA.

Step 7 – Developing the concept of operation (CONOP – Concept of Operation) and the operation plan (OPLAN – Operation Plan).

Step 8 – Assessing the campaign and revising the OPLAN.

The MDMP – Military Decision Making Process – represents the adapted analytical problem-solving model in the military. MDMP is an instrument serving the commander and his staff for developing estimates



and an action plan. While, formally, the problem-solving process starts upon receiving the mission and has the objective of elaborating an order, the analytical side of MDMP continues at all levels, throughout the entire operation. MDMP helps the commander and his staff acquire operational awareness and make logical decisions.

MDMP, as a whole, is a detailed, deliberate and time-consuming activity when there is enough time for planning and enough staff to elaborate as many likely own and enemy courses of action. This happens usually when the operation plan is being developed, when a new mission is being planned, during long-lasting operations, with a trained staff who knows the MDMP in depth. The advantages of going through the entire MDMP instead of an abridged version instead are the following:

- It analyses and compares numerous likely own and enemy courses of action in order to identify the most feasible own COA.
- It manages to reach the most comprehensive integration, coordination, and synchronization of an operation and minimizes the risk of omitting a critical aspect of the operation.
- It has as a result an order or a detailed plan.

The military decision-making process has seven steps. Each step starts with a trigger which, in turn, is represented by the end-state of the previous step. Each step has an end-product that contributes to conducting the following steps:

- Step 1* – Receipt of mission.
- Step 2* – Mission analysis.
- Step 3* – COA development.
- Step 4* – COA analysis.
- Step 5* – COA comparison.
- Step 6* – COA approval.
- Step 7* – Orders production.

2. Personal input

There are a lot of officers and NCOs who describe the MDMP using adjectives such as "very complex", "very difficult" or simply "too time-consuming". Frustration occurs especially late at night in the monologues of the chief of staff in the command post who is trying to bypass or shorten the MDMP and arguments for raising the efficiency of the process. The



question that derives from it is the following: Is MDMP a viable method of solving the current problems faced by the staff or is it time we came up with a different paradigm? What should MDMP ensure? Why is it so difficult to apply the process by the units? Which are the alternative processes? Are these alternatives viable? These are but a few of the questions we have in mind and which we are going to try to answer in this paper.

The main argument is that MDMP is hindered by linear, routine procedures that do not reflect natural cognitive processes and it proposes an alternative model based on six components developed concomitantly, derived from approaching the systems of problem-solving. We suppose that successful planning should not be perceived as progress by effectively going through the pre-defined stages, but as a change of the state of key attributes of planning models and operational environment; attributes such as the scope, uncertainty, precision, risk, resources, criteria and objectives. While pre-defined steps may be deceiving, these key attributes are always real and should be the grounds for decision-making. In other words, our planning model should be descriptive, not prescriptive. By trying to prescribe a series of activities, MDMP gives up the capacity to correctly describe the problem and the solutions proposed.

Readers familiarized with the latest provisions of the Planning Manual will probably admit the fact that many of the problems described in this paper are approached and there are attempts to solve them. The introduction of these cognitive models represents the special potential to improve the collective problem-solving capacity, but the current implementation is undermined by the attempts to synchronize the cognitive methods (which are strictly non-linear) with the old model of linear planning. The faulty interface between the two models, in our view, makes it all the more difficult to solve problems. The successful implementation of a new cognitive model depends on the development of a planning process that might support it and this article aims at presenting such a model.

It is true that MDMP works, at least partially, as a pre-defined instrument for decision-making in a short time, in certain circumstances. The conditions are as follows: objectives are pre-defined and very simple; a significant part of the plan is provided by the superior echelon as tasks and control measures for the operation; there is a period of inactivity, followed by a period of activity (the execution phase); the information flow is mainly



directed downwards, namely from the superior echelon towards the subordinates.

3. Defining the problem

During the latest decade, there have been a series of studies and research regarding the decision-making process, made by both the military and the business or the academic environment to the hope of optimizing the process. As it was stated above, MDMP is criticized as being time- and resource-consuming, unrealistic, dogmatic and difficult. MDMP is considered time-consuming because the deadlines until which certain issues have to be taken care of do not allow for covering the whole process. It is considered unrealistic because planners put the process into practice only if they are being subject to certification. It is also considered unrealistic because the decision-making process is full of uncertainty and, therefore, it is almost impossible to acknowledge all the information in order to choose the best solution to solve the problem.

MDMP is characterized as dogmatic because planners focus on the process instead of focusing on the result. Since MDMP is based on analysis to the detriment of synthesis, it can be subjected to criticism that it is a mechanic and rigid process. Is there an alternative to MDMP? The main argument of the majority of people who criticize this process is mostly based on the research made by Gary Klein. Gary Klein is a psychologist specialized in the study of cognitive processes pertaining to decision-making, who has made numerous studies in this field for US Army. He said that the army needs to adopt a limited type of reasoning within decision-making instead of a complex decision-making process based on analysis.

The issues are complex and it is often difficult to see the larger picture and always complicated by factors such as terrain, weather, technology or morale. Regardless of the complexity of the situation, conducting the fight seems to be a simple issue, and MDMP is a method of deciding how to use the available resources in order to solve a tactical issue.

The plans generated by MDMP are valuable only if they solve the respective problem. They are not automatically valuable, detailed, innovative, or daring, only if they have abided by the doctrine frame. In considering the value of MDMP, it is important to admit this central truth. The decision-making process is nothing but a way of solving the issues.



Doctrine terms or the overlapping of certain matrices and diagrams sometimes conceal this but, ultimately, the objective of any MDMP is solving a problem.

Anything replacing the current type of process needs to solve a large range of problems or issues, not only a particular one or a set of problems. A problem-solving methodology should be generally applicable, not to address only a single set of possible problems; otherwise its value is none. This intrinsic truth works for any field of activity, but all the more so in the military domain in which the general staff needs to solve complex problems, from a humanitarian operation to medium intensity military conflicts.

The MDMP used by the general staff should be applicable to all possible situations that might occur. MDMP is purposefully thought to have universal applicability. It is exactly this general applicability that inoculates frustration to those applying it. MDMP does not include details about the problem; it only provides the methodology of identifying the problem, generating possible solutions, analyzing them, comparing and determining the optimal solution. The commander and his staff have to use to maximum capacity their thinking.

It is no wonder that battalion and brigade staff are crying for help. The two major problems that the staffs confront when applying MDMP are the following: the lack of experience and a limited amount of training time working with this process. The lack of experience of commanders and staff is a problem that we need to admit, and the current organization of career courses curricula tends to partially solve this problem. We consider that, at least at battalions and brigade levels, this lack of experience will persist.

If we are making an assessment of infantry units, for instance, we can establish that the deficit of infantry captains available for being appointed in tactical units' commands should be a major concern for decision-makers in the management of human resources. The lack of personnel immediately results in this lack of experience. In many maneuver units, the positions with duties in planning are filled in with personnel covering a plurality of positions, without the necessary minimal training. The officers who have not gone through the stage of company commanders get to be appointed in planning positions.

At brigade level, there are a lot of situations in which planning positions, in all the functional staff domains, are filled with officers who



have not occupied company commanders' positions or who are not aware of the real issues of a battalion. The fact that these officers who are solely experienced in platoon level issues find MDMP as a real burden should not surprise anyone, but the lack of experience is not limited only to those who have or not gone through the company commander level. There are many officers who are very proficient at organizing and conducting practical activities but severely or even completely lack staff experience.

The general lack of experience in working with MDMP, from our point of view, is caused by the insufficient time allotted to personnel training. Daily routine, administrative issues, the extra-tasks and the much-blamed short deadlines for answering orders that become redundant often make it difficult to allocate temporary resources for training.

A possible solution would be that once appointed in a staff position, the young officer should participate in a dedicated workshop that might help him/her adjust easily to the specific aspects of the unit and to acknowledge his/her duties within MDMP. Yet, when the results of staff officers' work are not satisfactory, the commanders' options are to either accept their work or change them; going through the training program once again is simply unfeasible from the point of view of the budget and time allotted to this activity. The frantic rhythm of activities makes personnel training a requirement that limited resources are rarely capable to fulfill.

Taken as a whole, the combination of lack of people, lack of experience of the personnel and the limited amount of time available for training makes it even harder to go through the MDMP in a rapid and efficient manner. These issues are not new in the army, but they seem to become increasingly acute. All these factors place the battalion or brigade commander in a difficult position as he has to start wondering how he is going to manage with an untrained staff when they need to go through MDMP in the stress of the battle or during certification exercises.

Practice shows that there are three types of commanders' detrimental attitudes, namely: commanders who ignore the problem, ignore the process, or ignore the subordinated personnel. The most frequent attitude is ignoring the problem. The commanders who adopt this solution refuse to admit that the staff is not prepared to go through MDMP. In these units the commander has a reduced involvement and the chief of staff's involvement is only related to following the schedule, without paying any attention to the quality



of the work. The chief of staff is bound to be permanently dissatisfied with the quality of work produced by his/her staff but will not have enough time to redo the documents because of the compulsory nature of passing to the next MDMP stage.

The problem is that we have grown accustomed to rapidly going through the MDMP, without paying attention to a thorough analysis of the problem and the staff offers the commander recommendations for adopting a certain COA that is based on false assumptions and superficial analyses. When the commander approves COA, the staff will be in the position to redo many of the tasks because of being wrong and so on. Such orders may do a lot of harm in real situations. We do not believe that a certain staff is able to self-educate. We consider that they will also adopt the easy way out at the next exercise, that is why the only method to stop the phenomenon is to go through a training program with the whole staff. The conclusion we can draw is that ignoring the problem is not the answer.

The second attitude presented is ignoring the process in favor of choosing a way to avoid or completely replace MDMP by using operation orders already filled in, estimates, matrices, or statistics from other exercises that had been checked once and passed the quality test.

These instruments are useless when their limits become obvious. Each instrument of this kind has an authentic value as an MDMP supplement, but it cannot replace the MDMP. A useful example is the extended role of the targeting process used for performing seek and assault operations during tactical exercises.

From the doctrine point of view, the targeting process is a methodology through which the most efficient manner of using force multipliers within the structure of a maneuver unit. As the process involves completing a matrix, it is generally considered to be a task that might be rapidly executed. Some supporters of this process say that the targeting process can even be used for determining COA or the daily Fragmentary Order (FRAGO). By using the targeting matrix for identifying enemy targets and the neutralizing manner, an untrained staff believes to have identified a shortcut in the manner of elaborating the daily FRAGO.

This shortcut avoids elements that are important within MDMP and probably the most important one would be determining the decisive point. The decisive point is the place/moment in which the unit will concentrate



the effects of fire-power in order to obtain the expected results and it is also the first step in developing COA.

The targeting process, used as a replacement for MDMP, replaces the identification of decisive points with selecting one or several valuable targets. The targeting process has as an effect visualizing the enemy as a series of targets and synchronizing the allocated forces for eliminating a specific target. Within the targeting process, too little attention is paid to the synchronization of effort. Enemy attrition thus becomes the implicit solution in relation to it. The targeting process, when used as a replacement for MDMP, tends to make the unit focus on the annihilation instead of incapacitating the enemy. This does not mean that the targeting process has no value or it is flawed. It rather shows that the targeting process was designed to work within MDMP, not instead of MDMP. Units should use the targeting process for synchronizing organic force multipliers, instead of using it for selecting and developing a COA. Although the targeting session has become a constant part of MDMP, there are more than a few who support a more general applicability.

From our perspective, the applicability of the targeting process in the selection and development of COA is limited to a few types of operations. The truth is that no matrix, diagram, or pre-formatted slide can avoid the need for clear and analytical thinking in order to solve tactical problems. Matrices and other instruments can help the personnel a lot in managing, visualizing, and presenting information, but they cannot solve tactical problems; cognitive processes are those that can do so and shortcuts often generate more problems than they solve. The conclusion is that the optimal way of solving tactical issues is going through the whole MDMP and not using shortcuts.

The third attitude that more and more commanders adopt is ignoring the staff altogether. While the staff is going through the mental turmoil of MDMP, the commander goes to a quiet place and performs his own analysis. At the moment of presenting the decision briefing, the commander has already made up his own COA that he will disclose to the staff at the end of the briefing. Unfortunately, this will determine the staff to resume the whole process from the beginning. This is the so called MDMP of a single COA.



A number of authors have argued in favor of developing a single COA, after which the staff expose their estimates and go through the war games. This manner of conducting MDMP has as fundament the development of COA by the commander who is going to present it to the staff as a planning guide, preferably right after the mission analysis briefing. Although this manner of approaching the problem is not far from the rules and provisions, it is quite oddly put in practice, in the sense that it is quite frequent that the commander presents his COA quite late. Thus, although the staff need to adopt this COA and release operation orders, they do not have all the details, even if they are the entity that is going to subsequently conduct the operation and establish its efficiency.

In such cases, the commander may be the only person who truly understands the plan. The hazard of such an arrangement is quite obvious and it soon grows in significance, as the fatigue and perils on the battlefield will prevent the commander's direct involvement in combat. The existence of a staff is based on an objective necessity, namely that a single person cannot do everything by himself. In this sense, ignoring the staff is not a realistic solution.

4. A variant of adapting the current model

There is a series of elements that can be employed in order to decrease the *suffering* of the staff, which might simultaneously allow them to fulfill their role and assist the commander. When military thinkers established the MDMP steps, they identified and transposed all these stages in a scientific manner and included them in the planning manual; unfortunately, the units implementing these steps are quite rare.

The planning manual admits that personnel has to plan the operation under the pressure of time. According to this concept, almost all staffs at battalion or brigade levels conduct operational planning under the pressure of time. The inadequate level of training of personnel leads to a faulty conduct of MDMP. From our perspective, the commander can only help personnel in three ways when there are syncopes in conducting MDMP or there are time constraints. Thus, the commander may:

- increase direct involvement in the conduct of the process, thus offering personnel immediate confirmation from the most experienced tactician in the unit;



- offer more planning guidance, thus limiting the flexibility of personnel and maintaining them focused on the issues the commander deems as vital;

- limit the number of COA that need to be taken into account or direct personnel towards a specific COA.

By combining these options, the commander may obtain timely and quality analyses from the staff.

The direct involvement works in case the staff is made up of energetic, committed, yet untrained personnel. In time, the staff are going to become self-confident and will infer the commander's intent and the manner in which he tackles tactical problems. A commander who invests time and energy in training subordinates is going to be rewarded by them with high quality work and offering rapid and efficient solutions.

5. An alternative model to the military decision-making process

A common characteristic of all models is a certain classification. The decision-making and planning models are trying to separate in categories the elements of a problem and its solution, and the next six categories are proposed here, to our mind being the most solid and useful:

Step 1 – Operational environment – whatever exists, has existed and will exist.

Step 2 – Objectives – how we wish to influence the environment / threat / enemy.

Step 3 – Courses of Action (COA) – including operational design, methods.

Step 4 – Analyzing COA – how COA is going to influence the operational environment.

Step 5 – Evaluating COA – what value it has according to the objectives set.

Step 6 – Decision and execution – communicating COA to the structures that need to apply them.

These six components represent a planning model that, in time, has to be refined and adapted in order to increase its accuracy, to make it more precise and more efficient. We consider these components more military-system-friendly and we believe they are suitable for solving tactical problems or for decision-making.



The model based on six components presented here is the basis of a problem-solving process, generally valid, which might contribute to a series of models and methods that planners may resort to, also offering a common planning picture which is necessary for collaborative planning within and between organizations. MDMP is quite close to this basic model and it could be converted without significant disruption in the existing provisions.

However, there are certain important differences that make this model much more useful for the type of operational environment envisaged for future operations. The most important fact is that these components cannot be developed simultaneously.

6. Is it time to change the paradigm of the military decision-making process?

MDMP has not exceeded its usefulness; there is no other process that offers the universal possibility to solve problems. Although far from perfect, MDMP remains the best resource available for making tactical decisions. Moreover, from our point of view, we will not be able to solve the shortage of people or adequate training in the near future either. We will keep on having redundant tasks and we will not be able to allocate enough time for the integrated training of the staff.

Yet, it is time for a change! The commander's personal involvement in the planning, mentorship, teaching and training process can do a lot of things to compensate for the challenges faced by the battalion and brigade personnel nowadays. Increasing the commander's role in the planning process does not necessitate any change in the current doctrine; it is only a matter of proving more flexibility in applying the doctrine. Preparing and training an efficient staff is an immense and sometimes frustrating challenge. Only those commanders who are willing to invest time in training their staff will be able to make them realize that fighting means solving problems and this problem-solving is based on a game of thinking.



Bibliography

1. *** PO(2010)0143, “Comprehensive Approach Report”, 13 Oct 2010 and PO(2011)0045 “Updated List of Tasks for the Implementation of the Comprehensive Approach Action Plan and the Lisbon Summit Decisions on the Comprehensive Approach”, 7 March 2011.
2. *** AJP_5_Operational_level_planning_with_UK_elements, page 1-1, 2014 edition.
3. *** FM101-5_the military decision making process, page 5-3.
4. Mclamb Is it time to abandon the mdmp, page 99, MILITARY REVIEW 1 March-April 2002.
5. David L., Walker Refining the MDMP for Operational Adaptability, page 1, Small Wars Foundation, 2011.
6. Maj, John; J., Marr The Military Decision Making Process: Making Better Decisions Versus Making Decisions Better, Monograph, (Leavenworth: School of Advanced Military Studies, US Army Command and General Staff College, 2001).
7. A.D, Hall A Methodology for Systems Engineering, (Van Nostrand, 1962).



TANKS AND THEIR TACTICS, WHERE TO? 100 YEARS OF HISTORY

Brigadier General (ret.) Professor Gheorghe TOMA, PhD
Tenured member of Academy of National Security Sciences,
E-mail: gtoma49@yahoo.com

Abstract: *The 20th century was the real breakthrough in the history of humanity, the century marked by most scientific discoveries, which brought up new tendencies in the endowment and conduct of military actions. Each branch found reasons for being considered the “queen” of battles. The military historians of the time, and not only, made a series of rankings regarding the influence of these branches and categories of service, but actually each of them played a vital role in the fate of the conflicts which burst out throughout this century during which the largest number of people died, as man, with an indescribable ruthlessness, killed his peers. Not even nowadays is it clear where the conflicts started from or – and especially – who the winners were. Tanks and armored vehicles followed the same trends, they were developed and continuously improved and they determined a lot of tactical, operation and strategic level changes in their manner of employment. Nowadays they are irreplaceable on the battlefield, the best way of neutralizing a tank being the engagement of another; therefore, they need to be permanently modernized.*

Keywords: *tank, armored vehicle, tactical, operation, strategic, integrated, independent.*

The directions in which armored units and their tactics are heading would be easy to infer if the reasoning instruments were pretty clear and accessible enough, but we notice that this question may apply first of all to the very terminology we are using. We have to implement – as fast as possible – certain clarifications regarding the fate of armored troops nowadays when our country and therefore the army too are going through a transition period that requires investigations, tests, analyses which are so necessary in order to change directions, orient trends and plan for the future in military thinking and practice.



It is obvious that we cannot ignore the historic evolution of the phenomenon under study. At the respective moment, a Romanian officer was saying that the introduction of armored vehicles in the army is actually “a sign of civilization which has really become a necessity in all fields”¹.

A little later, Deygas wrote: “the appearance on the battlefield of mechanical vehicles on tracks is an event whose importance is only equaled by the invention of gunpowder”². Another Romanian officer was saying at that moment that tanks “are going to evolve so much that a lot of the tactical notions will be significantly amended”³.

Another prediction was confirmed after World War I when, in the Romanian military writings it was specified that: “the tank, due to its firepower, to its independent movement on the terrain, on the tactical field and its reduced vulnerability becomes a decisive weapon in the decisive phase of the attack”⁴.

The inter-war years represented a remarkable period for the army due to the special attention given to all branches and military specializations and especially to defining and redefining armored vehicles described, in turn, as: “auto terrain vehicles with armament or armor”⁵ “iron-clad auto vehicles, provided with armament and guns; they can easily move on the wrought-up terrain of the battlefield”⁶.

The after war period witnesses the “building of trucks for transporting troops in varied terrain, capable of ensuring protection of the mounted personnel against hostile engagement executed by the enemy with

¹ Cpt. C. Zaglaru , *Motorizarea armatei*, București, 1929, p. 5.

² F. C. Deygas, *Les chars d'assaut-leur passe, leur avenir*, Editura Charles – Lavauzelle, Paris, 1937, p. 338.

³ Mr. Polihram Dumitrescu, *Informații și legături cu transportul în automobile*, Tipografia militară, București, 1928, p.7.

⁴ Florea Țenescu, *Cunoștințe generale asupra războiului și studiul lui*, Tipografia Militară a Ministerului de Război, București, 1921, p. 100.

⁵ *Regulamentul provizoriu asupra întrebunțării tactice a marilor unități*, Editura Bacovia, I.E. București, 1939.

⁶ Gavrilescu A., Teodorescu Tr., *Conducerea trupelor*, Editura Cartea Românească, București, 1935, p. 123.



small caliber guns (...) in other words, the endowment of the infantry, artillery and other branches with armored vehicles"⁷.

Given the aspects presented above, we may state that, from the action point of view, armor units have an heterogeneous endowment, they are supported by other branches and categories of armed forces (helicopters, aviation, anti-tank defense means) and, while accomplishing combat missions, they act according to the principles of *joint arms combat*, with the peculiarities and combat procedures specific for the respective tactics, also known as "*armored troops tactics*"⁸, as a category that contributes to constituting the general tactics of land forces.

After World War II, the introduction of armored vehicles in the Romanian army knew a vast process of modernization. The new requirements of the battlefield, oversaturated with military technique, determined the directions of action for building fighting machines (tanks) in order to be able to cope with the new circumstances, the essential assets being considered general organization, mobility, firepower and their protection. Tanks were thus re-defined and called "*the main striking force*"⁹ of land forces due to the following reasons: they act simultaneously with helicopters (pertaining to joint actions), they are protected by air defense and anti-armor accompanying means; they are used concurrently and act by surprise; they can continue the fight day and night or in circumstances of reduced vulnerability; they can use in different stages of the battle those technical means allowing them to reach a high pace of advance, whether they act independently or in cooperation with other branches.

The experience of the two world wars, the lessons learned from the exercises conducted with armored units show that both independent actions and the integrated actions require, on the one hand, conceiving the battle doctrine in connection to the steps made by the reform in the army and, on the other hand, developing the tank tactics (both theoretical and applied), the

⁷ General-maior Gh. Stănescu, col. ing. Dumitru Vochin, *Tancuri și automobile*, Editura Militară, București, 1978, p. 173.

⁸ Col. dr. Valentin Arsene și colectiv, *Cerințe doctrinare ale perfecționării tacticii*, Editura Militară, București, 1982, p. 64.

⁹ The term *striking* is used in order to mark the moment when strike reaches enemy formation (author's note).



armored units being an integrating factor of all arms due to their qualities proven during its 100 years of evolution.

Through the transformation of the Romanian army, the structures endowed with armored vehicles preserve their dominant position, having the possibility to combine firepower with tactical capability. The supremacy of tanks was not preserved as such without any issue. They had to confront a large range of weapons, high-tech ammunition, artillery projectiles, mines, all of them capable to annihilate them. Besides, mention should also be made of the hostility manifested by their traditional enemies.

Tanks and armored vehicles were never invulnerable, and the periodic predictions regarding their being rendered obsolete were erroneous because they were based on a mistaken concept of tank. We need to acknowledge the fact that armor makes tanks immune to a lot of assault weapons and special weapons are needed to destroy them, reason for which they have high survivability on the battlefield.

Although tanks could always be destroyed, they continue to be efficient for two reasons: the first is the fact that the ratio between the threats they have to face, such as anti-tank and other kinds of weapons and their survivability has not changed substantially; the second reason is that no weapon system except for the tank is able to play the role it plays together with the armored structures. Tanks and armor structures that include tanks in their organics make up a unique combination of assault force and resistance in place force. Actually it was tank units that decided the fate of battles and even campaigns during World War II and the most recent campaigns in the Middle East.

Lately, there have been a series of revolutionary developments regarding tanks and armored vehicles generally speaking. The first was determined by the introduction in the '60s of guided anti-tank missiles, which forced tanks to rely more on cooperation with other arms, which highlights the importance of using them in integrated actions or for independent actions as such. The second consists in introducing in the army endowment helicopters with missiles, having as a result a higher mobility of anti-tank means than that of tanks themselves. This led to an increased difficulty in concentrating and maneuvering tanks structures increasing at the same time the need for self-defense means of tank structures.



The future is going to bring us also other revolutionary achievements, through which tanks are going to be able to face attacks from all directions, including vertical ones, in other words benefitting from an omni-directional protection that might influence the result in their favor. A great change has also taken place regarding the basic concept of tank. The concepts of light, medium, and heavy tank were replaced with the concept of tactical mobility tank, operative mobility tank and strategic mobility tank.

All these changes are going to make armored forces be in the position to continue to fulfill the demands of war-waging principles, tanks remaining the very spine of land forces.

Although there have been various attempts coming from various directions at diminishing their importance, due to the lack of other means capable of their performance, they are going to continue to represent an interest for tacticians and builders.

In the future, the efficiency of tanks has to be supported by conceiving a flexible doctrine. The units participating in the future conflicts pictured by military thinkers as a combination of heavy, light, and special forces, a structure made up of active and reserve elements, will need to place tanks as a reference factor for the whole concept of preparing and conducting land forces actions.

The recent military conflicts (events) display a completely new image of the dimensions of armored protection, namely a perfect combination of three features: the destructive power of the armament, the mobility and capacity of protection against enemy fire. Maximal efficiency presupposed: integrating tactics, techniques and procedures, the speed of adaptation on the battlefield to the concrete conditions and the quality of transmission means.

“Walking alone in our existence as tankers, permanently intertwining fear and joy, we are going to know, when time comes, how to be – for any of the possible aggressors – a continuous surprise in a strange silence”¹⁰.

¹⁰ Col. prof.univ.dr. Toma Gheorghe, *Blindatele moderne. Studiu de artă militară*, Editura Academiei de Înalte Studii Militare, București, 1998, p. 133



Bibliography

1. Valentin, Arsene și colectiv *Cerințe doctrinare ale perfecționării tacticii*, Editura Militară, București, 1982.
2. Deygas F. C. *Les chars d'assaut-leur passe, leur avenir*, Editura Charles – Lavauzelle, Paris, 1937.
3. Gavrilescu, A.; Teodorescu, Tr. *Conducerea trupelor*, Editura Cartea Românească, București, 1935.
5. Gheorghe, Toma *Blindatele moderne. Studiu de artă militară*, Editura Academiei de Înalte Studii Militare, București, 1998.
4. Stănescu, Gh.; Dumitru, Vochiu *Tancuri și automobile*, Editura Militară, București, 1978.
6. Țenescu, Florea *Cunoștințe generale asupra războiului și studiul lui*, Tipografia Militară a Ministerului de Război, București, 1921.
7. Zaglaru, C. *Motorizarea armatei*, București, 1929.



MAINTENANCE OF PUBLIC ORDER – BETWEEN SCIENCE AND ART

Professor Țuțu Pișleag, PhD
E-mail: tutu.pisleag@yahoo.com

“There is no happiness without freedom, no freedom without self-governance, no self-governance without constitutionalism, no constitutionalism without morality; in turn, each of these progress features cannot exist without stability and order”

Clinton Rossiter

Abstract: *The purpose of this paper is to analyze the concepts of maintaining, ensuring and restoring public order as enshrined in the national laws in relation to i) the need for a professional model of policing, and ii) to the model of the continuum of force use, given the conditions for the existence of the two public order enforcement entities – the police and the gendarmerie. The method of analysis is focused on examining and inter-connecting the content of public order strategies issued by the Ministry of Internal Affairs, the laws regarding the scope of the public policy dimensions of maintaining, ensuring and restoring it, and whether these reflect the reality of the public space in Romania. The present paper also approaches the elements of continuity in the development of the strategies, the extent to which they are implemented and if the public order domain is divided on three sub-areas (maintaining, ensuring and restoring it) to justify the current employment of the public order forces.*

Keywords: *police, gendarmerie, public order, professional police model, prevention, strategies.*

The qualitative analysis of the content of strategies¹ developed by the Ministry of Internal Affairs for enforcing order and public security clearly

¹ *Strategy of the Ministry of Administration and Interior for achieving order and public security in order to increase the citizen’s safety and prevent street crime, Romanian Official Gazette no. 243 of 23 March 2005; National Strategy of Public Order 2010 - 2013, Romanian Official Gazette no. 721 of 28 October 2010; National Strategy of Order and Public Security 2015-2020, Romanian Official Gazette no. 763 of 13 October 2015.*



shows that at strategic level there have been and still are instruments and visions meant to consolidate public security in Romania and at the same time reflect the reality of the operational situation regarding criminality at national level. From the point of view of the concept, it includes three notions: maintaining public order², ensuring public order³ and re-establishing public order⁴, which were implemented after the '90s and which are still used nowadays. Yet, they are rather focused on delimiting the attributes and competences of police and gendarmerie. Also, the Ministry of Internal Affairs elaborated the Strategic Institutional Plan of the Ministry of Internal Affairs 2014 - 2016⁵ which specified the challenges to law and order, among which "the emergence of crimes atypical for the Romanian background, such as bank robberies, mugging by means of fire arms,

² *Public Order Maintenance* represents all the measures, activities and actions organized and conducted daily by the order and public security forces, in order to ensure the normal functioning of state institutions, protect and respect the citizens' fundamental rights, civic norms, social behavior rules, as well as the other supreme values and the public and private wealth, *Strategy of the Ministry of Administration and Interior for achieving order and public security in order to increase the citizen's safety and prevent street crime*, Romanian Official Gazette no. 243 of 23 March 2005, line. 3.1.

Public Order Maintenance represents all the measures, activities and actions organized and conducted daily by the police, in order to ensure the normal functioning of state institutions, protect and respect the citizens' fundamental rights, civic norms, social behavior rules, as well as the other supreme values and the public and private wealth, *National Strategy of Public Order 2010 – 2013*, Romanian Official Gazette, Part I, no. 721 of 28 October 2010.

³ *Ensuring public order* comprises all the measures taken for enforcing the law, the prevention and deterrence of actions aiming at social turmoil or violent acts during public meetings and demonstrations, cultural and sports activities, as well as other similar manifestations with numerous participants; this is ensured by main and support forces according to competences, *Strategy of the Ministry of Administration and Interior for achieving order and public security in order to increase the citizen's safety and prevent street crime*, Official Gazette no. 243 of 23 March 2005, line 3.1.

⁴ *Re-establishing public order* refers to the legal measures taken in order to restore it to the initial state in case it has been seriously disturbed, with peaceful means or through the exclusive use of force, *Strategy of the Ministry of Administration and Interior for achieving order and public security in order to increase the citizen's safety and prevent street crime*, Official Gazette no. 243 of 23 March 2005, line 3.1.

⁵ *Annex to Order of the Minister of Internal Affairs* no. 159 of 05.11.2014.



kidnappings, sequestrations, gun thefts, organized crime (terrorism, people trafficking, drug trafficking) and ... cross border crime, taking diverse and complex shapes (illegal migration, illegal piloting, forgery, trafficking counterfeit goods..."⁶. As for the concepts of ensuring and restoring public order, we consider that they actually represent the right to public meeting and freedom of expression, which has to be protected, actually a concentration in space and time of a certain public, in a certain context that claims the operationalization of a proactive strategy appropriate to these hot "spots".

*

As public order is also considered an "element of national security", we may state that we are facing a fundamental desideratum of the rule of law state.

The three notions: maintaining, ensuring and restoring public order were also among other things a reason for promoting the two laws in the field, Law no. 60/1991 regarding the organization and conduct of public meetings (reissued) and Law no. 61/1991 for sanctioning the breaking of certain norms of social conduct and public order (reissued). In a democratic society, public order becomes a desideratum, a demand, and an imperative necessity, the state being responsible for providing the public order climate in the society, circumscribed to public safety. Moreover, along its evolution, each state has developed its legal norms and the necessary structures for applying the law depending on its own historic, political, social and cultural peculiarities etc. and irrespective the nature of the law enforcing agencies (public order forces or public security forces) it is essential that human rights be respected, so as to ensure a public order climate within parameters accepted and claimed by the society for consolidating the rule of law.

At UN level, within the Code of Conduct for Law Enforcement Officials⁷ it is stipulated that they "fulfill the duty imposed upon them by law, by serving the community and by protecting all persons against illegal acts, consistent with the high degree of responsibility required by their

⁶ *Institutional Strategic Plan of the Ministry of Internal Affairs 2014 – 2016 (annex to the Order of the Minister of Internal Affairs no. 159 of 05.11.2014)*, p. 14.

⁷ *Code of Conduct for Law Enforcement Officials*, Adopted by General Assembly resolution 34/169 of 17 December 1979.



profession. "⁸ The respective text is accompanied by the comment according to which "In countries where police powers are exercised by military authorities, whether uniformed or not, or by State security forces, the definition of law enforcement officials shall be regarded as including officers of such services"⁹. Thus, we may consider the police and the gendarmerie as law enforcement agencies (institutions) and their personnel as law enforcement officials, but it is even more interesting that the duties of the gendarmerie are purely police-like and most therefore be reconsidered, although the gendarmerie is "a specialized military institution...".

Another issue regarding the complexity and challenges specific to public order stems from the National Strategy of Defense for 2015 – 2019, which are shown within the lines of action in the public order dimension¹⁰ and which are circumscribed as an essential constitutional objective of social life. If we take into consideration the imperative concept of strategies providing *public order and security* then certainly "this approach is an integral part of acknowledging security [safety] as a public or common commodity that has to be produced in common by all those involved and which guarantees the rights and freedoms of all citizens"¹¹, but especially

⁸ Art 1, *Code of Conduct for Law Enforcement Officials*, Adopted by General Assembly resolution 34/169 of 17 December 1979.

⁹ *Ibidem*.

¹⁰ Increasing the security of citizens by protecting the life, bodily integrity, and their right to property; identifying and countering the activities conducted by trans-border organized crime networks and disrupting criminal groups; preventing and combating tax evasion and other forms of economic-financial criminality; combating drug consumption and trafficking; securing the boundary, especially that which is the external boundary of the European Union, in order to combat illegal migration, people trafficking and other risks with an impact upon national security; increasing the response and management capacity of emergency situations; increasing the level road and transport safety and transportation; ensuring human resources, material, financial, and informational means necessary for maintaining and developing the operational capacity of institutions with duties in this regard based on a rigorous planning process, *National Defense Strategy of the Country for the period 2015 – 2019. A Strong Romania in Europe and in the World*, Romanian Official Gazette, 23 June 2015.

¹¹ Maurice Chalom, Lucie Léonard, Franz Vanderschueren, Claude Vézina, *Urban Safety and Good Governance: The Role of the Police*, UNCHS - Habitat, ICPC, 2001, p. 35.



that *co-production* at the tactical and operation levels of law enforcement agencies.

Keeping in mind all the above, from a theoretical perspective and through inter-connection with the daily reality, we may state that public order is much more comprehensive than its expression in legal norms, which makes it become a major issue for national security. Operationalizing national strategies and departmental leads us to a different conclusion according to which maintaining public order actually is basically an operational tactics equally relying on science and art. From the perspective of complexity, fluidity, dynamics, content and physiognomy of public order we notice that it is impossible to "create a law, a rule, or a regulation that might take into account each possible variable in a rapidly developing situation, with a potential of violence"¹². This is exactly what inculcates the assumption that here we are dealing with the organic relation between art and science in the operational tactics of maintaining public order. the operational tactics also outlines another aspect, namely that of effects at strategic (national) level and not only at the tactical level as such, the local level. Thus, the authority and legitimacy of public order forces are strengthened in the citizen's perception that he/she is protected, taking into account the fact that they are authorized and have the capacity to resort to violence, embracing and even emphasizing the idea that "the protection of constitutional rights is the mission of police in a democracy"¹³. Although, from the perspective of the content of these strategies reflecting the dimensions of public order, we notice that at the level of public order management, of adopting operational tactics and their results, expressed mainly through the citizen's perception upon their degree of safety, there are some imbalances that become much more visible in punctual critical situations of engaging public order forces.

¹² Chuck Canterbury, *Reasonable force isn't perfect force: Opposing view*, <https://eu.usatoday.com/story/opinion/2017/07/10/reasonable-force-perfect-force/103589682/>.

¹³ Sue Rahr, Stephen K. Rice, *From Warriors to Guardians: Recommitting American Police Culture to Democratic Ideals, New Perspectives*, in *Policing Bulletin*, Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2015. p. 2.



When we refer to science we actually refer to "principles, rules, concepts and methodology"¹⁴, norms, procedures integrated with other sciences. In this domain of public order, science presupposes "understanding those aspects (...) of tactical and technical capabilities and of the procedures – which may be measured and coded"¹⁵. Art, on the other hand, implies the specialized performances of specific abilities based on intuitive qualities, experience, training, good judgement, capability and capacity to integrate them, creativity and flexibility, most of the time in tense emergency of uncertainty circumstances, in the unique circumstances of a given situation, with the vital need for preparation or information assessment of the action area. In the same manner, art also implies the integrating capacity of all these elements and not only, which in painting would represent the different combination of the same colors with the end state of a masterpiece and less with naive painting.

Taking into account the three concepts, or levels of public order – maintenance, ensuring and restoring – we may state that the latter two, ensuring and restoring have no continuity in time and space, but they rather presuppose a density and action intensity related to certain events, which actually pertain to public order maintenance rather focused on ensuring public safety. Major attention has to be paid to the level of maintenance of public order, resulting in the imperative need for a professional police model (including the gendarmerie), for a model of public order, actually a continuum of the use of force that might express police actions in the public space, according to those consecrated in other police systems – *local community police, police oriented towards felonies and crimes and the police based on / conducted by information*. As for the community police which is rather a philosophy than a police strategy, although it is approached differently as neighborhood policy or police of proximity, we may identify

¹⁴ Gheorghe Văduva, *Știința militară. Rolul științei militare în managementul mediului de securitate și apărare în procesul de modernizare a societății*, Universitatea Creștină „Dimitrie Cantemir”, Institutul de Studii de Securitate, 2011, p. 3.

¹⁵ ADP 3-90, *Offence and Defence*, Army Doctrine Publication No. 3-90, Headquarters Department of the Army Washington, DC 13 august 2018, article 1-22.



"three common strategies: partnership relations police-community, a problem solving approach and organizational decentralization"¹⁶.

*

We consider that at the level of conceptualization of public order strategies at national level, the concepts settled are those of maintaining, ensuring and restoring public order rather determined through the legal differentiation by law of the police and gendarmerie duties, in a social context particularly characterized by the democratic transformation of the society without further studying the content and evolution of public order and security, of a completely changing and dynamic operational reality connected to the crime situation outside national borders. In our viewpoint, the three concepts of maintaining, ensuring and restoring public order which are used nowadays were adopted and implemented in an uncritical manner and without keeping in mind the fact that police forces, through their policing mission essential to such a service, have to be adapted to the Romanian society they are serving. In other words, it was rather necessary to come back to rural gendarmerie because nowadays we witness increasingly difficult and controversial approaches to "achieving public order and safety". The assessment of strategies in the field of public order does not result in an explicit model, nor do they use a certain police model, actually a mixture of models, based on police adjustment and approach specific to Romanian society. Taking over and implementing the concept of police of proximity as a structure, as being valid for any police service, led to leaving aside the preventive patrols, directed patrols, or routine patrols which had proven their efficiency and this demonstrates the fact that nowadays we need to rethink the manner of ensuring public safety and the duties of the gendarmerie as police force.

The functions of police and gendarmerie forces have to be understood first and foremost through the daily activity of maintaining public order and these two forces have to be rather proactive "than a reactive force that responds to the already committed crimes. They need to act in a proactive entity within a large range of circumstances that tend to disturb

¹⁶ Peter Somerville, *Understanding Community Policing*, Policing An International Journal of Police Strategies and Management, May 2009, University of Lincoln, UK, p. 5.



the peace of the community or negatively affect the quality of life"¹⁷. This is actual prevention, otherwise the public order forces may be considered not to have gone over "the popular model of fighter against crime which is a reminiscence"¹⁸ of the beginning of police activity. Both institutions, the police and the gendarmerie, are destined exclusively to a police service and public order can be considered as a domain in the area of expertise and authority of the public order forces, police and gendarmerie.

The research in the field identified the strategic approach of the professional model of *problem solving police* that aim at the "causes of the problems behind a long line of criminal incidents"¹⁹ to the detriment of the professional model of *incident-driven police* in which "directions are oriented towards solving individual incidents instead of solving the recurring problems caused by crimes"²⁰. Within this model, "directions are oriented towards solving individual incidents"²¹. The strategic approach of the problem-solving oriented police model practically influences everything that the police do, as well as the gendarmerie, both operationally and from the management point of view and implies four principles²²:

- using extensive knowledge about the local environment in order to identify criminal patterns, often associated with certain areas, that may be defined as a problem in the scanning phase;
- collecting and analyzing as much information as possible about a certain problem (from both internal and external sources) to the purpose of understanding the causes of an identified problem (analysis phases);

¹⁷ Edwin Mees, *Community Policing and the Police Officer, Perspectives on Policing*, National Institute of Justice, U.S. Department of Justice, January 1993 No. 15, p. 2.

¹⁸ *Ibidem*.

¹⁹ Anthony A. Braga, *Problem - Oriented Policing and Crime Prevention*, 2nd edition, Criminal Justice Press

Monsey, New York, U.S.A., 2008, p. 12.

²⁰ *Ibidem*, p.10.

²¹ *Ibidem*.

²² Jennifer West, *Problem-Oriented Policing: A Team Approach, National Overview on Crime Prevention*, Conference proceedings series. Canberra: Australian Institute of Criminology, 1992, p. 196.



- investigating the nature of the answer that might solve the basic problem through the analysis of conditions and factors of a problem that will subsequently lead to the implementation of a potential solution through the development of a series of possible alternatives, viewed as an answer to the basic problem. As the causes of most crimes go beyond the normal borders of policework, the development of solutions would usually involve other institutions and, in many cases, the community at large (response phase);
- assessing the implemented solutions, so that, if the response failed, it has to be adjusted (modified) by improving the analysis and, in some cases, by redefining the nature of the problem.

At the same time, we have to bring into discussion the fact that such a strategic approach becomes efficient in crime prevention and combating if police forces are "too focused on police *means* and neglect the *objectives* of crime prevention and control as well as other community problems"²³.

The implementation of such a strategic approach in police affairs is sure to cause a fundamental change of the professional model of policemen that, besides the measures of "crime prevention, maintenance of order, applying sanctions, arrests, etc., thus include mediation, negotiation, inter-relations with other institutions, with the community. Still, more important than changing competences is changing attitudes: instead of reacting to incidents, the policeman analyses, plans and takes initiative. Instead of permanently resorting to bureaucratic command mechanisms for guidance and assistance, the policeman has to solve the problem to the best interest of the community²⁴. This vision is also supported by David Couper's observation²⁵ regarding the activity of the policeman who "sees the activities of a town through the window shield of a police car and listens to

²³ David Weisburd, Cody W. Telep, Joshua C. Hinkle, John E. Eck, *The Effects of Problem Oriented Policing on Crime Goldstein and Disorder*, Campbell Systematic Reviews, 2008, p. 4.

²⁴ Edwin Mees, *Community Policing and the Police Officer, Perspectives on Policing*, National Institute of Justice, U.S. Department of Justice, January 1993 No. 15, p.2.

²⁵ Chief of Madison Police Department (1972 – 1993); he contributed to implementing „community police”, including what became known as „Madison method” of controlling the mob. <https://isthmus.com/news/news/former-mpd-chief-david-couper-takes-modern-policing-to-task/>.



the town's actions through a police radio. These are rather restrictive opinions of urban life". The strategic approach described above is among other recognized as a "proactive approach of the police that aim at the main causes of problems."²⁶

Beside the police approach oriented towards problem solving combined with the information-based police, "sometimes there may be included traditional police tactics and new technologies of information and communications"²⁷ with the purpose of prevention in which patrolling is considered a fundamental police practice even if it is one of the most time and resource-consuming tasks. Still, it is demonstrated that "in certain circumstances, the active police presence and its high visibility in a community may reduce the crime rate because people change their behavior if they perceive a great probability of being sanctioned (being placed under arrest)."²⁸

In conclusion, we consider that prevention is a fundamental anticipatory function in the domain of public order which, in our opinion, should represent the strategic objective of public order forces and, at the same time, be a relevant assessment criterion. It has already been demonstrated that "it is crime prevention that is essential, not the arrests made"²⁹ and the slogan that "the task of the police is to catch thieves" is obsolete as it places the law enforcement forces in a reactive situation. This does not mean that they have to give up sanctioning anti-social deeds, but rather prevention has to become a priority, which is the only way to increase the level of citizen's trust in law enforcement forces. Regarding the notions of providing and restoring public order as were included at first also in the gendarmerie competences in this domain, we consider that the result is a fracture of legal protection of public order as it is difficult to ensure public order during public meetings when maintaining public order in the same

²⁶ United Nations Office on Drugs and Crime, *Training Manual on Policing Urban Space*, United Nations Office at Vienna, February 2013, p. 24.

²⁷ *Ibidem*, p. 2.

²⁸ Sarah Lawrence, Bobby McCarthy, *What Works in Community Policing? A Best Practices Context for Measure Y Efforts*, The Chief Justice Earl Warren Institute on Law and Social Policy University of California, Berkeley School of Law, November 2013, p. 6.

²⁹ Tamara Rise Lave, Eric J. Miller, *The Cambridge Handbook of Policing in The United States*, Cambridge University Press, 2019, p. 36.



public space pertains only to the police. In this respect, the strategic approach of the renowned notion of "information-based police"³⁰ produces operational malfunctions during public meetings while gendarmerie forces are periodically involved in these actions, in the organization and conduct of public meetings, be they spontaneous or not. This approach implies collecting specific information at all levels that, analyzed and connected to information technology provides fundamental support to planning, organizing and conducting operations of public order maintenance. We may even talk about the concept of *public order intelligence*. Given the aspects presented above, we consider that the conceptual and operational approach of public order forces' engagement through the artificial breaking up of the competences of maintaining, ensuring and restoring public order, in circumstances in which maintaining public order is a priority. In this respect, there is a need to rethink areas of expertise and authority of the two law enforcing forces by connecting them with the traditional characteristic features of the area of action, be it urban or rural. Thus, if we deal with the duties of the gendarmerie that are mainly circumscribed to ensuring and restoring public order, duties that do not have a daily character in space and time in an area of responsibility, we need to reconsider the functions of the gendarmerie in the domain of public order maintenance by criteria and characteristics of the action space, urban or rural (gendarmerie posts, gendarmerie stations). Under these circumstances, there would be a growing capacity of action for providing police services to the benefit of the citizen and community.

Thus, there is an imperious need to reconsider the nature of gendarmerie duties as purely police duties, considering the domain of public order in the area of expertise and authority of public order forces, police and gendarmerie. Beyond all these, there is a need for changing organizational culture, supporting and promoting professionalism at all organizational levels, although in reality "changing the culture of a department may be equally difficult if not even more difficult than changing policies,

³⁰ The origins of this concept lie in 1980 – 1990 in Great Britain, due to the increase of criminal activities. Jerry H. Ratcliffe, *Intelligence-led Policing*, Trend & Issues in Crime and Criminal Justice, No. 248, Australian Institute of Criminology, April 2003.



procedures and instruction"³¹. By taking into consideration the manifestation of violence, in any society, as part of human experience, in all its shapes and "despite the fact that violence has always been present, it is not to be accepted by the world as an inevitable part of human condition, its prevention should be viewed as a priority"³², there is a need for a professional police model in which emphasis falls on the selection (recruitment), admission, initial training, life-long learning and career evolution. With respect to initial training and life-long learning, curricula has to be re-thought by connection to the reality of the operational space and, concretely, training has to integrate fundamental subject matters in the field and *physical training* (physical abilities in defensive tactics, intervention, using means of protection and intervention, armament) with elements of training in (tactical) communication and behavioral management on the dynamics of use of force continuum model in circumstances in which the use of force represents significant challenges both for the institution and at individual level. A real reform at the level of public order forces should not affect only the constitution of mixed patrols (police forces and gendarmerie) but rather result in institutional decentralization (at the level of Ministry of Internal Affairs), rethinking the concepts of maintaining, ensuring and restoring order, in which maintaining public order is a priority given its attributes of primacy and which could be consolidated through operationalization of the *gendarmerie stations (posts)*, re-assessment of initial training and life-long learning.

The concept delineation on the three areas of expertise – maintenance, ensuring and restoring public order – is rather simplistic because of the co-existence of police and gendarmerie which actually triggered this ranking of an extremely dynamic and complex field in which maintaining public order from this perspective as an operational tactics is actually essential. We also consider that public order seen as a "territorial

³¹ Sarah Lawrence, Bobby McCarthy, *What Works in Community Policing? A Best Practices Context for Measure Y Efforts*, The Chief Justice Earl Warren Institute on Law and Social Policy University of California, Berkeley School of Law, November 2013, p. 12.

³² Jonathan Blanks, *Thin Blue Lies: How Pretextual Stops Undermine Police Legitimacy*, Case Western Reserve Law Review, Volume 66, Issue 4, 2016, p. 945.



legal concept"³³ has multiple facets and the definitions of this concept may be considered as satisfactory and pragmatic, specific to a "plurality of the normative environments in which they act". This may become much clearer by promoting a *law of public order* because "it is always difficult to define legal concepts without being able to verify their applicability in the field"³⁴. In this regard, we may mention the definition used in Romania according to which "public order, as an integral part of national security, is the state of legality, balance and peace, corresponding to a socially acceptable level of respecting legal norms and civic behavior, which allows the practice of constitutional rights and freedoms, as well as the functioning of the structures specific for the rule of law state and are characterized by the credibility of institutions, public health and morals, the state of normality in organizing and conducting political, social, and economic activities, according to the legal, ethical, moral, religious and other nature norms generally accepted by society"³⁵. Thus, the concept of public order is a pluralistic, multi-dimensional, evolutive and multifaceted one, whose content is directly determined by law on the basis of the standards of morality and public health, the need for safety of goods and people, and the practical applicability of this concept is only verified through the responsibility, high performance and credibility of police service. In this regard, even if until now reforms have been fragmented and hard to accept, reality proves the need of a modern management of police service, on the whole, to which the citizen is a beneficiary as a consumer.

Ensuring and restoring public order, as they are defined at strategic level, show a character of discontinuity in time and space, which actually represents and intensity and density of actions and operations determined by the dynamics of maintaining public order. Likewise, maintaining public order is often misunderstood for – most of the time – the organizing

³³ Țuțu Pișleag, *Ordinea publică – un concept juridic teritorial*, Revista Academiei de Științe ale Securității Naționale, nr. 2, 2017, p. 80.

³⁴ Marc Rémy, *Le maintien et le rétablissement de l'ordre public par la police: définitions, acteurs et principes juridiques*, Revue économique et sociale: bulletin de la Société d'Etudes Economiques et Sociales, vol. 66 n°2 Juin 2008, p. 27.

³⁵ *Strategy of the Ministry of Administration and Interior for achieving order and public security in order to increase the citizen's safety and prevent street crime*, Romanian Official Gazette no. 243 of 23 March 2005.



structures of public order, (maintaining public order) and which is rather connected to the competences of sanctioning and fining. Actually, if we regard maintaining public order as operational tactics, we may say that public safety as it is defined³⁶ and by connection to constitutional provisions³⁷ is a fundamental right and one of the conditions for exercising individual and collective freedoms. Yet, to consider public safety – as it was specified in the 2005 strategy – as "expressing the feeling of peace and confidence conferred by the police service" is somehow mistaken because public safety implies a control of hazards and circumstances which lead to physical challenges, psychological challenges or physical damage at the level of the person or the group. At the same time, public safety also implies an objective dimension "defined by objective behavior and environment parameters"³⁸ and a subjective dimension "evaluated according to the feeling of safety (or unsafety) of the population"³⁹.

Furthermore, the present article also opens the debate for specialists to consider gendarmerie as a state police force, as its duties are purely police work. It is somewhat difficult to also accept the level of public order restoration, obviously in the vision of public order strategies, as it may be considered as a course of expressing maintenance and ensuring public order, most of the times because of a faulty management of public meetings, irrespective of their nature. Here we are also referring to the experience of public law enforcement forces regarding the "intervention competences which should be considered optional, not compulsory... and not be used

³⁶ Public security refers to the feeling of calm and confidence conferred by police service in order to apply methods of maintaining peace and public order, the degree of security of people, gatherings, and goods, as well as for achieving the civil society – police partnership, to the purpose of solving community issues, defending human rights, freedoms, and legal interests of the citizens, Decision no.196 of 17 March 2005 regarding the approval of *Strategy of the Ministry of Administration and Interior* for achieving order and public security in order to increase the citizen's safety and prevent street crime, Romanian Official Gazette no. 243 of 23 March 2005.

³⁷ *Chapter II, Title II, Romanian Constitution*, Romanian Official Gazette, issue 233 of 21 November 1991 (modified and completed, Romanian Official Gazette, issue 767 of 31 October 2003).

³⁸ *Safety and Security Promotion: Conceptual and Operational Aspects*, https://www.inspq.qc.ca/pdf/publications/150_SecurityPromotion.pdf.

³⁹ *Ibidem*.



automatically"⁴⁰. During initial training and life-long learning, there is a need for acknowledging and acquiring the standards and principles of applying the rule of law, emphasizing more the attitude and presence of law enforcing forces in which tactical communication (dialogue) might be a priority also from the reasonable use of force.

The domain of law enforcing forces would also be a priority in institutional reform, in a unitary, integrated, and modern perspective at national and European level, meant to reconsider both the content of tactical training and the attitude towards it, based on professional discipline which may be accomplished through understanding the motivation that truly drives those who intend to become police officers.

Bibliography

1. *** *Constituția României*, Monitorul Oficial nr. 233 din 21 noiembrie 1991 (modificată și completată, Monitorul Oficial nr. 767 din 31 octombrie 2003).
2. *** *Legea nr. 60/1991 privind organizarea și desfășurarea adunărilor publice*, Monitorul Oficial al României, Partea I, nr. 192 din 25 septembrie 1991, republicată, Monitorul Oficial al României, Partea I, nr. 505 din 4 iunie 2004.
3. *** *Legea nr. 61/1991 pentru sancționarea faptelor de încălcare a unor norme de conviețuire socială, a ordinii și liniștii publice*, Monitorul Oficial nr. 196 din 27 septembrie 1991, republicată.
4. *** *Strategia națională de apărare a țării pentru perioada 2015 - 2019, O Românie puternică în Europa și în lume*, Monitorul Oficial nr. 450 din 23 iunie 2015.
Strategia Ministerului Administrației și Internelor de realizare a ordinii și siguranței publice pentru creșterea siguranței cetățeanului și prevenirea criminalității stradale, Monitorul Oficial nr. 243 din 23 martie 2005.
5. *** *Strategia națională de ordine publică 2010 - 2013*, Monitorul Oficial, nr. 721 din 28 octombrie 2010.

⁴⁰ Jim Murdoch, Ralph Roche, *The European Convention On Human Right and Policing, A handbook for police officers and other law enforcement officials*, Council of Europe Publishing, December 2013, p. 108.



6. *** *Strategia națională de ordine și siguranță publică 2015-2020*, Monitorul Oficial nr. 763 din 13 octombrie 2015.
7. *** *Planul Strategic Instituțional al Ministerului Afacerilor Interne 2014 – 2016* (anexă la Ordinul ministrului afacerilor interne nr. 159 din data de 05.11.2014).
8. *** *Strategia Ministerului Administrației și Internelor de realizare a ordinii și siguranței publice, pentru creșterea siguranței cetățeanului și prevenirea criminalității stradale*, Monitorul Oficial nr. 243 din 23 martie 2005.
9. *** *Code of Conduct for Law Enforcement Officials*, Adopted by General Assembly resolution 34/169 of 17 December 1979.
10. *** United Nations Office on Drugs and Crime, *Training Manual on Policing Urban Space*, United Nations Office at Vienna, February 2013.
11. *** *ADP 3-90, Offence and Defence*, Army Doctrine Publication No. 3-90, Headquarters Department of the Army, Washington, DC 13 august 2018.
12. Jonathan, Blanks *Thin Blue Lies: How Pretextual Stops Undermine Police Legitimacy*, Case Western Reserve Law Review, Volume 66, Issue 4, 2016.
13. Anthony A., Braga *Problem - Oriented Policing and Crime Prevention*, 2nd edition, Criminal Justice Press Monsey, New York, U.S.A., 2008.
14. Maurice, Chalom; Lucie, Léonard; Franz, Vanderschuren; Claude, Vézina *Urban Safety and Good Governance: The Role of the Police*, UNCHS – Habitat, ICPC, 2001.
15. Sarah, Lawrence; Bobby, McCarthy *What Works in Community Policing? A Best Practices Context for Measure Y Efforts*, The Chief Justice Earl Warren Institute on Law and Social Policy University of California, Berkeley School of Law, November 2013
16. Edwin, Mees *Community Policing and the Police Officer, Perspectives on Policing*, National Institute of Justice, U.S. Department of Justice, January 1993 No. 15
17. Jim, Murdoch; Ralph, Roche *The European Convention On Human Right and Policing, A handbook for police officers and other law enforcement officials*, Council of Europe Publishing, December 2013.
18. Țuțu, Pișleag *Ordinea publică – un concept juridic teritorial*, Revista Academiei de Științe ale Securității Naționale, nr. 2, 2017.



19. Sue, Rahr; Stephen K., Rice *From Warriors to Guardians: Recommitting American Police Culture to Democratic Ideals*, New Perspectives, in Policing Bulletin Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2015.
20. Jerry H., Ratcliffe *Intelligence-led Policing*, Trend & Issues in Crime and Criminal Justice, No. 248, Australian Institute of Criminology, April 2003.
21. Marc, Rémy *Le maintien et le rétablissement de l'ordre public par la police: définitions, acteurs et principes juridiques*, Revue économique et sociale : bulletin de la Société d'Etudes Economiques et Sociales, vol. 66 n°2 juin 2008.
22. Tamara, Rise Lave; Eric J., Miller *The Cambridge Handbook of Policing in The United States*, Cambridge University Press, 2019.
23. Peter, Somerville *Understanding community policing*, Policing An International Journal of Police Strategies and Management, May 2009, University of Lincoln, UK.
24. Gheorghe, Văduva *Știința militară. Rolul științei militare în managementul mediului de securitate și apărare în procesul de modernizare a societății*, Universitatea Creștină „Dimitrie Cantemir”, Institutul de Studii de Securitate, 2011.
25. David, Weisburd; Cody W., Telep; Joshua C., Hinkle; John E., Eck *The Effects of Problem Oriented Policing on Crime Goldstein and Disorder*, Campbell Systematic Reviews, 2008.
26. Jennifer, West *Problem-Oriented Policing: A Team Approach, National Overview on Crime Prevention*, Conference proceedings series. Canberra: Australian Institute of Criminology, 1992.
27. *** <https://eu.usatoday.com/story/opinion/2017/07/10/reasonable-force-perfect-force/103589682/>.
28. *** <https://isthmus.com/news/news/former-mpd-chief-david-couper-takes-modern-policing-to-task/>.
29. *** https://www.inspq.qc.ca/pdf/publications/150_SecurityPromotion.pdf.



NATURAL DISASTERS, A GROWING HAZARD FOR WORLDWIDE STATES

Colonel Associate Professor Engineer Florin NEACȘA, PhD
Tenured Member of the Academy of National Security Science,
E-mail: neacsaf@yahoo.com

***Abstract:** Natural disasters are manifest differently all over our planet, most of them displaying a violent nature and producing many victims among the population, as well as sometimes very significant economic damages. The current article was meant to emphasize the types of natural disasters and which were their consequences in 2018 as compared to the last 10 years. One can notice that their manifestation is tightly related to global warming, which is affecting our planet and leads to a violent action of a series of disasters such as: floods, vegetation fires, drought and storms. Another type of natural disaster which caused many victims and produced major material damages in 2018 was the earthquake. This is a type of natural disaster that has a stronger and stronger manifestation also in Europe, specialists running lately a series of studies regarding morbidity associated with post-earthquake periods.*

***Keywords:** natural disasters; vegetation fires; earthquake; morbidity; victims; economic damages.*

The Research Center for Epidemiology of Disasters (CRED) has been conducting its over 40 years of activity in the field of international studies regarding disasters and conflicts occurring everywhere in the world. CRED supports activities of research, training and technical expertise in the domain of humanitarian emergency situations – placing special emphasis on activities regarding assistance and counseling, rehabilitation of affected regions and durable development. The center was set up in 1973 in Bruselles, within the Public Health School of the Catholic University in Louvain (UCL) and, according to Belgian laws, it is a non-profit institution with an international statute.

Starting with 1980, CRED collaborates with World Health Organization (WHO), being an integral component of the Global Program for Readiness and Emergency Response of WHO. This favored the development of CRED international network, through permanent cooperation with numerous UN agencies, inter-governmental and



governmental institutions, different nongovernmental organizations, numerous research institutes or universities. In 1988, CRED launched EM-DAT- the database regarding worldwide disasters, made up on sponsorship received from the Bureau of External Assistance with Disasters (USAID / OFDA) of United States Agency for International Development. EM-DAT comprises important data regarding the occurrence and effects of over 14,000 natural disasters and 8,400 anthropic disasters, produced at global scale since 1900 up to the present day. EM-DAT specialists divide natural disasters in several sub-groups as follows: geophysical (earthquakes, mass movement (dry), volcanic activity); hydrological (floods, landslides, wave erosion); meteorological (storms, extreme temperatures, fog); climatological (drought, ice lakes flooding, wildfire); biological (epidemics, epizooties, zoonoses and insect-caused infections); extra-terrestrial (objects falling from the space, natural space phenomena).

The data held by EM-DAT specialists show the fact that, on global level, in 2018, there were 315 natural disasters. These resulted in the deaths of 11,804 people; over 68 million people were affected and economic loss amounting to 131.7 billion US dollars¹. The most affected continent was Asia, where 45% of the whole number of events were reported, leading to the death of 80% of all the deaths of people at global scale and 76% people being affected of all, worldwide. From the point of view of the affected states, a highly different situation in the world is Indonesia, that marked 47% of the total number of deceased people and India, with 35% of the entire number of affected people². Regarded from the perspective of the sub-groups presented above, most people who died were because of earthquakes (45% of the number of deaths) and floods (24% of the number of deaths)³. Most people were affected by floods (50% of the whole number of affected people) and storms (28% of the entire amount of affected people), were also on the Asian continent. A considerable contribution to these high percentages was given by the fact that Asia is a very large continent, population is more numerous in comparison to the other continents and the risks of various disasters is particularly high.

¹ file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.

² file:///D:/Downloads/CredCrunch54%20(1).pdf.

³ file:///D:/Downloads/CredCrunch54%20(1).pdf.



In comparison to the yearly average of the last ten years (2008-2017), we can notice that the number of natural disasters is smaller, 315 (in 2018) as compared to 348 which is the annual average of the period 2008-2017. The number of deceased people, 11.804 (in 2018) as compared to 67,572 which is the annual average of the period 2008-2017, as well as in the case of affected people, over 68 million people (in 2018) as compared to 198.8 million people that is the annual average of the period 2008-2017, and the value of economic loss is 131.7 billion USD (in 2018) as compared to the 166.7 billion USD which is the annual average of the period 2008-2017⁴. This is a good aspect, but we must take into account the fact that in 2018 there were no catastrophic disasters such as the earthquake in Haiti, in 2010, when 222,500 people died, the drought in India which, between 2015 and 2016, affected 330 million people, or the earthquake in Japan, followed by the tsunami in 2011 which caused economic damage amounting to 210 billion USD.

Of all the types of natural disasters, the one that caused the most deaths among the population, in 2018, was the earthquake (actually a number of violent earthquakes) in Indonesia, in August and September, causing 4,904 deceased people or missing people⁵. Moreover, in 2018, there numerous wildfires (10 such events) as well as a significant volcanic activity (7 such events), that produced a lot of victims as well as significant, and even historical, economic damage. In this sense, for instance, the wildfire that happened in Greece, Attica region, in July 2018 caused the death of approximately 100 people, this being the most deadly fire produced in Europe, as shown by the EM-DAT entries⁶. Another wildfire, which was very violent happened in November 2018, in California, USA, known as Camp Fire and considered the deadliest (86 dead people) and most costly in the history of California state⁷. At the same time, it is the sixth deadliest wildfire of all the data to be found in the USA and the economic damage estimated at approximately 16.5 billion dollars is the highest ever marked in

⁴ file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.

⁵ file:///D:/Downloads/CredCrunch54%20(1).pdf.

⁶ https://en.wikipedia.org/wiki/2018_Attica_wildfires.

⁷ [https://en.wikipedia.org/wiki/Camp_Fire_\(2018\)](https://en.wikipedia.org/wiki/Camp_Fire_(2018)).



the USA⁸. Volcanic activity was especially intense in 2018, resulting in a larger number of deaths than that in the last 18 years. In this sense, we can talk about the eruption of volcano Fuego in Guatemala, situated 44 km away from Guatemala City, which happened on June 3rd, 2018, and which caused the death of over 400 people, affecting a total amount of over 1.7 million people⁹. Another devastating eruption occurred on December 22nd, 2018, when volcano Anak Krakatau from Indonesia erupted and the landslide produced a devastating tsunami which affected Java and Sumatra islands, resulting in 426 dead people and 14,059 injured people¹⁰.

Hydrological natural disasters, and especially floods are the most devastating natural disasters worldwide due to the number of people affected and the economic damage produced. In 2018 there were 127 such events, the most destructive of which being the floods in August 2018 in India, Kerala state, which caused the death of 504 and specific issues for over 23 million people. Abundant rains led to devastating floods in Nigeria causing the death of 300 people and affecting approximately 2 million people, while in Japan floods resulted in the loss of 230 human lives, these being the biggest loss since 1982 up to the present day¹¹.

In 2018, the largest economic loss was caused by meteorological natural disasters; thus, in the USA, Florence and Michael hurricanes caused material damage worth of 30 billion USD and Jebi typhoon caused in Japan material damage worth of 12.5 billion USD. Other countries were also affected by severe storms, such as China and India, while in the Philippines there were over 300 people dead and over 10 million people affected¹².

We should also mention the fact that a series of natural disasters also affected the countries already affected by military conflicts, such as: in Somalia (a country frequently affected by drought) floods affected 700,000 people; in Afghanistan the drought affected over 3.6 million people; in Kenia, drought affected 3 million people; in Central America, over 2.5

⁸ https://en.wikipedia.org/wiki/List_of_natural_disasters_by_death_toll#Deadliest_wildfires/_bushfires.

⁹ https://en.wikipedia.org/wiki/2018_Volc%C3%A1n_de_Fuego_eruption.

¹⁰ https://en.wikipedia.org/wiki/2018_Sunda_Strait_tsunami.

¹¹ [file:///D:/Downloads/CREDNaturalDisaster2018%20\(2\).pdf](file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf).

¹² *Ibidem*.



million people were affected by drought; in Madagascar drought 1.2 million people¹³.

At global level, in 2018, the repartition of natural disasters on continents is as follows: the most numerous ones were in Asia, 141 such events, and from the point of view of countries, the most numerous events were reported in India and China – 22 disasters for each – Indonesia, 15 natural disasters, Philippines, 10 natural disasters, Japan and Vietnam, 7 disasters each, Afghanistan, 6 natural disasters, Myanmar, 5 natural disasters; the next continent from the point of view of natural disasters is America, most of them being reported in the USA – 19 natural disasters – and Argentina – 5 natural disasters; then the European continent, with 48 natural disasters reported, most of which being in France – 7 such events; while Africa reported 46 natural disasters and Oceania, 15 such events¹⁴.

Another extremely interesting comparison refers to the number of natural disasters occurring in 2018 depending on the sub-groups established by EM-DAT specialists, refers to the annual average of 2008-2017 decade. Thus, we have the following data: climatological ones (draught, 16 in 2018 as compared to 17 which is the annual average of the period 2008-2017, wildfires, 10 in 2018 as compared to 9 which is the annual average of period 2008-2017); geo-physical ones (earthquakes, 20 in 2018 as compared to 26 which is the annual average of the period 2008-2017; mass movements (dry), 1 in 2018 as compared to 1 which is the annual average of the period 2008-2017; volcanic activity – 7 in 2018 as compared to 4 which is the annual average of the period 2008-2017); the hydrological ones (floods – 127 in 2018 as compared to 153 which is the annual average of the period 2008-2017; landslides – 13 in 2018 as compared to 19, which is the annual average of the period 2008-2017); the meteorological ones (extreme temperatures - 26 in 2018 as compared to 20 which is the annual average of the period 2008-2017; storms – 95 in 2018 as compared to 101 which is the annual average of the period 2008-2017)¹⁵.

Following the same ranking of natural disasters, the statistics of people deceased in 2018, on types of disasters as compared to the annual

¹³ file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.

¹⁴ *Ibidem*.

¹⁵ *Ibidem*.



average during 2008-2017, show the following figures: climatological ones (drought, 0 in 2018 as compared to 2004 which is the annual average of the period 2008-2017, wildfire, 221 in 2018 as compared to 80 which is the annual average of the period 2008-2017); geophysical ones (earthquakes, 5264 in 2018, as compared to 35,197 which is the annual average of the period 2008-2017; mass movements (dry), 17 in 2018 as compared to 24 which is the annual average of the period 2008-2017; volcanic activity, 878 in 2018 as compared to 44 which is the annual average of the period 2008-2017); hydrological ones (floods, 2,879 in 2018, as compared to 5,039 which is the annual average of the period 2008-2017; landslides, 275 in 2018 as compared to 1,034 which is the annual average of the period 2008-2017); meteorological (extreme temperatures, 536 in 2018, as compared to 7,388 which is the annual average of the period 2008-2017; storms, 1,734 in 2018 as compared to 16,762 which is the annual average of the period 2008-2017)¹⁶.

The countries with most deceased people, in 2018, were Indonesia with an amount of 5,357 (from different sources: 4,340 because of earthquake followed by tsunami, 564 because of earthquake and 453 because of volcanic activity followed by tsunami), India with 453 dead people because of floods and Guatemala with 425 people dead because of volcanic activity¹⁷.

The number of people affected by natural disasters in, depending on types of disasters, in comparison with the annual average of the period 2008-2017, are as follows: climate (draught, 10.8 million people in 2018 as compared to 73.8 million people, which is the annual average of the period 2008-2017; wildfire, 0.3 million people in 2018, as compared to 0.1 million people, which is the annual average of the period 2008-2017); geophysical (earthquakes, 1.4 million people in 2018 in comparison with 8.3 million people, which is the annual average of the period 2008-2017; mass moves (dry), 0 in 2018 as compared to fewer than 0.1 million people, which is the annual average of the period 2008-2017; volcanic activity 1.8 million people in 2018 in comparison with 0.2 million people which is the annual average of the period 2008-2017); hydrological (floods 34.2 million people in 2018

¹⁶ file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.

¹⁷ file:///D:/Downloads/CredCrunch54%20(3).pdf.



as compared to 73.1 million people, which is the annual average of the period 2008-2017; landslides fewer than 0.1 million people in 2018 as compared to 0.3 million people, which is the annual average of the period 2008-2017); meteorological (extreme temperatures 0.3 million people in 2018 as compared to 9.0 million people, which is the annual average of the period 2008-2017; storms 19.4 million people in 2018 as compared to 33.9 million people, which is the annual average of the period 2008-2017)¹⁸. We notice a significant increase in the values in case of climate natural disasters, but only regarding wildfire and geophysical fire, through the high volcanic activity.

Of all the people affected by disasters at global level, we notice that in 2018, the highest number of affected people was in Asia with 76.3 %, as compared to the annual average of the period 2008-2017 which is 79.8 %, the second position is occupied by Africa with 12.6 % in 2018, as compared with 9.2 % which is the annual average of the period 2008-2017, on the third position we find America with 9.8 % in 2018, as compared with 10.5 % which is the annual average of the period 2008-2017, the fourth place is occupied by Oceania with 1.2 % in 2018 as compared to 0.3 % which is the annual average of the period 2008-2017, while on the fifth position we find Europa with 0.1 % in 2018 as compared to 0.3 % which is the annual average of the period 2008-2017¹⁹. The repartition on countries of the number of people affected by natural disasters shows us that the most affected country in 2018 was India with 23.2 millions of people affected by floods, followed by the Philippines with 3.8 million people affected by typhoon Mangkut, Afghanistan with 3.6 million affected by drought, Kenya with 3.0 million people affected by drought and China with 2.5 million people affected by storms²⁰.

The economic loss, at world level, in 2018 as compared to the annual average between 2008 and 2017, are thus distributed in percent: the biggest percent in 2018, of 53.0%, is found in the two American continents, as compared to 44.1% which is the annual average between 2008 and 2017, followed by Asia with 42.1% in 2018 as compared to 45.1% which is the

¹⁸ file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.

¹⁹ *Ibidem*.

²⁰ *Ibidem*.



annual average between 2008 and 2017, on the third position we find Europe with 2.3% in 2018 as compared to 6.6%, which is the annual average of the period between 2008 and 2017, the fourth place is occupied by Africa with 1.5% in 2018 as compared to 0.6%, which is the annual average between 2008-2017, and the fifth place is Oceania with 1.0% in 2018 as compared to 3.5% which is the annual average between 2008 and 2017²¹.

The distribution of economic loss in 2018, on types of disasters, as compared to the annual average between 2008 and 2017, is the following: the climatologic ones (drought, 9.7 billion USD in 2018 as compared to 8.3 billion USD, which is the annual average between 2008 and 2017; wildfires, 22.8 billion USD in 2018 as compared to 3.8 billion USD, which is the annual average between 2008 and 2017); the geo-physical ones (earthquakes, 7.1 billion USD in 2018 as compared to 45.3 billion USD which is the annual average between 2008 and 2017; movements of dry land, 0 in 2018 as compared to less than 0.1 billion USD, which is the annual average between 2008 and 2017; volcanic activity 0.8 billion USD in 2018 as compared to less than 0.1 billion USD which is the annual average between 2008 and 2017); the hydrological ones (flooding 19.7 billion USD in 2018 as compared to 36.3 billion USD, which is the annual average between 2008-2017; landslides of dump land 0.9 billion USD in 2018 as compared to 0.3 billion USD, which is the annual average between 2008-2017); the meteorological ones (extreme temperatures 0 in 2018 as compared to 3.0 billion USD, which is the annual average between 2008 and 2017; storms 70.8 billion USD in 2018 as compared to 69.6 billion USD, which is the annual average between 2008 and 2017)²².

The most affected countries from the point of view of economic loss were the United States, amounting to 46.5 billion USD (16.5 billion USD due to wildfires, 16 billion USD due to hurricane Michael and 14 billion USD due to hurricane Florence) and Japan, amounting to 22 billion USD (12.5 because of typhoon Jebi and 9.5 billion USD because of floods)²³.

²¹ file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.

²² *Ibidem*.

²³ *Ibidem*.



From the data presented by EM-DAT specialists, we notice that geophysical disasters, namely earthquakes, resulted in the highest number of victims in 2018. The causes were the unpredictability of these types of disasters, the short period when they happened, and the devastating impact upon the environment. Although specialists in the field are studying the phenomenon in depth, at present there is no prediction regarding them and thus, their impact is quite different and characterized by a series of elements, of which the most important are: the size of manifestation (magnitude or intensity, depending on the scale used); the time of day when it happens (during the day or at night); the period of the year when it happens (depending on the season); the type of buildings existing in the respective area (from the point of view of the codes of seismic codes). All these things determine a great involvement of the political and decision-making factor at national and local level, of the specialists in the health field and of those managing such emergency situations.

The existing data in EM-DAT database show the fact that, between 2000 and 2017, in the world there were 504 earthquakes, 34 of which occurring in Europe (specialists took into account those whose average magnitude was 5.7 on Richter scale). The earthquakes happening in Europe, in that period, occurred in 13 different countries, the most affected being, in decreasing order, Italy, Greece, Spain, Serbia and Great Britain, and caused 701 deceased people, 257,303 affected people, and economic damage amounting up to approximately 29 billion USD²⁴. A significant feature was the fact that of the 34 earthquakes which happened in Europe during that interval, almost half, namely 15, had a magnitude higher than 6.0 on Richter scale. Between 2000 and 2017, Italy was the country in Europe most affected by this type of disaster (the earthquake in 2012 in Emilia Romagna region, that in 2016 which affected Amatrice town, that in 2009 in L'Aquila region), causing 679 deceased people and other 124,000 affected people. Economic losses were 27,665 million USD. Next in line is Greece with 8 deceased people and 82,701 affected people, and material damage worth 648 million USD. Spain had 10 deaths and other 15,300 affected people, economic loss being estimated at 217 million USD; Serbia had 2 people deceased and 27,030 affected people, while economic loss was valued at

²⁴ file:///D:/Downloads/CredCrunch51%20(3).pdf.



148 million USD; although Great Britain did not report any fatalities, it still reported 4,501 affected people and economic loss valued at 71 million USD²⁵.

Obviously, most people deceased because of earthquakes resulted from getting caught under collapsed buildings. At the same time, there were victims suffering from major or minor trauma, determined by falling or being caught under pieces of constructions tumbling down or with burns caused by the possible fires which might occur in such situations. The specialized personnel intervening in such emergency situations together with medical personnel have as priorities saving the victims, sorting and evacuating them and providing emergency assistance to different victims depending on the kind of trauma they have been affected by. Analyses made by specialists in the field show that earthquakes are directly responsible for the high number of victims, but, at the same time, they generate multiple health issues prolonged by the fact that population is moved to and sheltered in crowded places or camps where different diseases might occur among survivors, some of which contagious, where nutrition issues might occur among victims, many of which being manifested also after the emergency aspect has been solved²⁶.

If along the years specialists were mainly concerned with the impact of earthquakes on the area where it happens, through the destructions it might produce, lately specialists have started to be concerned with the impact of earthquakes on the population affected from the perspective of public health, taking into consideration the fact that there is less knowledge about the morbidity generated by earthquakes.

Thus, a lot of epidemiological studies have been made lately upon the affected populations and considered vulnerable after an earthquake and long-term results showed the occurrence of mental issues, cardio-vascular disorders, as well as a series of other chronic diseases.

Losing relatives or friends, losing one's house or its severe damaging, disrupting access to public or private services increase the risk of mental disorders of survivors because of post-traumatic stress. The studies made showed that the mental health of the children affected by a natural

²⁵ file:///D:/Downloads/CredCrunch51%20(3).pdf.

²⁶ *Ibidem*.



disaster was severely affected, resulting in a verbal intelligence much lower than that of other children of the same age who had not gone through such trauma. Furthermore, a study conducted in 2009, confirmed by another recent study, showed the fact that mortality due to cardio-vascular diseases at women and men survivors in a certain area is considerably higher than in the pre-disaster period (specialists consider that this may be caused by the increase in systolic pressure or hyper-glycemia after the disaster)²⁷.

All these studies have the role to reduce the current and future risk in case of earthquake, by introducing preventive strategies, which might considerably reduce mortality and morbidity in case of such a natural disaster. In this respect, the most important aspect is related to the training of the population; this falls into the responsibility of the political decision-makers, specialists in emergency situations and those in the health sector.

Research studies in the respective field are currently being conducted by CRED in cooperation with the University in L'Aquila, that has as a purpose evaluating the impact upon population of the earthquake in 2009, with respect to the types of diseases following it and the resulting mortality. In order for these studies to be as complete as possible, CRED is also cooperating with University Hospital in Tribhuvan (Nepal), through a research project that studies the impact of the devastating earthquake in 2015, from the point of view of people admitted in hospitals on types of diseases and ways of functioning²⁸.

Conclusions

If we make a brief outline of year 2018, the most significant natural disasters that happened along the year, we notice: earthquakes in Indonesia, floods in India, storms in Japan, a high number of wildfires and volcanic activities. The low number of deceased people, as compared to the annual average of the last decade may be attributed also to the increase in the level of protection of the population due to the measures adopted by the political decision-makers, in cooperation with specialists in the field, regarding the impact of climatic change.

²⁷ file:///D:/Downloads/CredCrunch51%20(3).pdf.

²⁸ *Ibidem*.



Wildfires occurred in a violent manner in the last years producing numerous victims and significant material damage. Their occurrence, most of the time, was lately favored by the canicular periods manifested during long intervals of time and with especially high temperatures that occur evermore frequently because of global warming affecting our planet. The countries in the South of Europe were confronted with especially violent wildfires – entire woods caught fire – but this was a high risk for any of the countries of European Community.

When one Member Country of European Union requires international support for such intervention, member countries send support such as tanker planes, helicopters especially equipped for such situations, intervention equipment and especially trained firemen. This request is fulfilled by activating the civil protection mechanism at the level of European Union, by the affected country, the intervention being coordinated from the level of Emergency Response Coordination Center (ERCC) of European Commission.

In 2017, forest wildfires in Europe led to the activation of the protection mechanism for 18 times, the most affected member states being Portugal, Italy, France, Montenegro and Albania²⁹. Also in 2017, U.E. offered international support to Chile (upon its demand), for quenching the most powerful wildfires in the history of this country. In 2018, wildfires determined the activation of the mechanism for five times, upon requests from Sweden, Greece, Portugal and Latvia³⁰. For the interventions in 2018, 18 tanker-planes were used together with 6 helicopters, 69 intervention trucks and over 400 firemen and pilots, and the satellite mapping system Copernicus of the EU, used for managing wildfires, generated 139 maps that offered especially important data regarding the surface covered, the intensity and amplitude of damage³¹.

Given the risk to earthquake which is extremely high for Bucharest, the city with the most exposed population – according to specialists – to earthquakes systematically produced in the same source (the seismic region Vrancea), because of its geographic positioning at a distance of

²⁹ file:///F:/Downloads/MEMO-15-5411_RO.pdf.

³⁰ *Ibidem*.

³¹ *Ibidem*.



approximately 150 km from the epicentral region Vrancea, which is also the approximate depth of Vrancea earthquake hotbed, in 2018 this was the spot where national exercise “SEISM 2018” was conducted.

This exercise had as purpose training the leadership structures and the response structures for taking appropriate action in case of a major earthquake (with a magnitude of 7.5 on Richter scale) which supposedly affected Bucharest in a major way and led to numerous victims among the population (actually, what was checked was the manner of applying “National Post – Seism Response Concept”). In order to conduct an exercise as close to reality as possible, a reality in which many Bucharest hospitals would be affected, simultaneously with the conduct of “SEISM 2018” national exercise, there was an international medical exercise. “ModEx 2018” was meant to – through our country’s requiring international medical support, by triggering the civil protection mechanism of the European Union – check the medical EMT 1-3 modules.

Bibliography

1. *** file:///D:/Downloads/CREDNaturalDisaster2018%20(2).pdf.
2. *** file:///D:/Downloads/CredCrunch54%20(3).pdf.
3. *** file:///D:/Downloads/CredCrunch51%20(3).pdf.
4. *** https://en.wikipedia.org/wiki/2018_Attica_wildfires.
5. *** [https://en.wikipedia.org/wiki/Camp_Fire_\(2018\)](https://en.wikipedia.org/wiki/Camp_Fire_(2018)).
6. *** https://en.wikipedia.org/wiki/List_of_natural_disasters_by_death_toll#Deadliest_wildfires/_bushfires.
7. *** https://en.wikipedia.org/wiki/2018_Volc%C3%A1n_de_Fuego_eruption.
8. *** https://en.wikipedia.org/wiki/2018_Sunda_Strait_tsunami;
file:///F:/Downloads/MEMO-15-5411_RO.pdf.



ARTIFICIAL INTELLIGENCE AND ITS IMPACT ON SECURITY

Colonel Ion-Marius NICOLAE, PhD

Land Forces Staff,

E-mail: marius24nicolae@yahoo.com; marius71nicolae@gmail.com

Motto:

"Artificial intelligence is fantastic, but it lacks, and it is always going to lack in something that only natural intelligence has on its side: a soul".

aphorism by **George Budoï** din "Aforisme" (15 februarie 2019)

Abstract: This article shows that artificial intelligence (AI) is an area of informatics that explores intellectual capabilities with computing devices and what its implications are for security.

Artificial intelligence (AI) is the ability of machines or computers to perform tasks normally associated with the human mind.

In computer science, artificial intelligence (AI) is the intelligence displayed by machines, unlike natural intelligence, displayed by humans and some animals.

Informatics defines the research of artificial intelligence as a study of "intelligent agents": any device that perceives its environment and performs actions that maximize the chance of successfully achieving its objectives.

The term "artificial intelligence" is used colloquially to describe machines imitating the "cognitive" functions that people associate with other human minds, such as "learning" and "solving problems"¹.

The term "artificial intelligence" first appeared in the year 1956 at a seminar at Stanford University in the United States of America.

Artificial intelligence is a technology with revolutionary potential for many sectors of activity.

In recent years, artificial intelligence has developed rapidly, serving as a basis for numerous computer applications in domains such as: healthcare, car industry, finance and economics, video games, military, auditing, advertising, art, education, space exploration, etc.

Nowadays, artificial intelligence is increasingly being used in the field of security and defense, especially in the cyber area, but also in security services.

¹ https://www.ro.w3ki.com/artificial_intelligence/, accessed on 10.09.2019.



In the field of security and defense, it is not too difficult to see why the use of artificial intelligence can represent both an opportunity and a hazard.

Keywords: *intelligence, artificial intelligence, learning machines, computers, security, defense.*

Introduction

Even if it seems to pertain to science fiction, *Artificial Intelligence (AI)* is a notion that appeared in ancient times.

The history of artificial intelligence – technology able to think as a human being – started in the second half of the 20th century.

Starting with the invention of the digital computer in 1940, researchers began to think more and more about the idea of constructing an artificial, electronic intelligence.

Thus, in the summer of 1956, during a workshop at American College Dartmouth, there were scientists who lay the foundation of research in Artificial Intelligence.

Unfortunately, though, at the beginning of 1970s, this research in Artificial Intelligence was abandoned as it was considered that researchers and their sponsors realized the technological limitations.

The interest in research and sponsorship for Artificial Intelligence were resumed at the beginning of the 1980s.

In the first years of the 21st century, investments and interest in Artificial Intelligence reached a peak and they have not decreased since then.

In the 21st century, it is quite obvious that people need to be able to answer to a higher and higher number of security alerts. Taking into consideration the speed at which cyber-attacks have spread in the entire world, starting with 2017, the answer needs to be very fast.

Confronted with the lack of relevant specialists in the world, companies also transform study machines in instruments of artificial intelligence for automatizing security processes.

In the context of security of information, Artificial Intelligence is an *“intelligent digital system that studies by itself; it develops systems of research and learning by itself; it may even have an own language (without being understood by people); it develops artificial neuronal networks by*



itself; it may write its own programs; most importantly, it has power of decision”².

Thanks to AI, it is now possible to predict and detect threats in order to prevent the possible cyber-attack. Thus, Artificial Intelligence may consolidate security in the real world as well as cyber-security.

Artificial Intelligence is a technology with revolutionary potential for many sectors, such as: health, car industry, finance and economics, video games, army, security, audit, advertising, art, education, exploration of space etc. Nevertheless, one of its main sectors in which it is successfully used is that of security and especially that of cyber-security.

1. Artificial intelligence – aid to the security teams

In the 21st century, companies have already started to use artificial intelligence in order to recognize and respond to security threats. At present, in the world, companies have sufficiently powerful instruments, but their managers need to decide as fast as possible to include them in the cyber-security of their companies.

1.1. Using Artificial Intelligence for detecting threats

Artificial Intelligence is used by the company Barclays Africa in order to detect signs of compromising the system in the local network. At the same time with the rapid change in the global threats and the increasing number of cyber-attacks, there is a need for processing a huge amount of data they need to face using the most advanced techniques and technologies to counter.

Cadence Design Systems, a company of engineering services, implemented a system of continuous monitoring of threats in order to contribute to protecting its copy right. The daily data regarding traffic security, coming from 30,000 desktops and 8,200 users is of approximately 30-60 GB and the analysts of the company studying it are only 15 in number. And this is not everything. The same company also stated that, in order to increase the number of analyses made, it is necessary to introduce artificial intelligence instruments in order to detect and solve the problems.

² <http://www.laurageorgescu.ro/inteligenta-artificiala-si-impactul-ei-societate/>, accessed on 11.09.2019.



Aruba Networks, a branch of Hewlett Packard Enterprise (*HPE*)³, uses relevant products in order to monitor the behavior of the user and the system, as well as to manage access to Cadence. As Cadence specified, a feature of Aruba platform is that it works according to the principle of self-learning. The company keeps adding, the attacks change and become more and more difficult: for instance, if for some time there has been an ill-intentioned activity of stealing data, which will further on give the hacker the possibility to steal a large amount of data and the instruments of automatic learning /artificial intelligence will contribute to its timely detection.

Even small companies are affected by the overload of security data. For instance, Daqri, a firm augmented for producing glasses and protection helmets, hires 300 people and only one person for the security structure. On the other hand, the processes of analysis and response to security events are highly time-consuming.

Using artificial intelligence from Vectra Networks in Daqri, approximately 1,200 people can be monitored in traffic. Automatized instruments may be observed when somebody scans hubs, goes from one host to another or, let us say, in an unusual manner sends somebody large quantities of data. The company collects all relevant information, analyzes them and introduces them in the self-learning model. This makes it possible to prevent the possible malware incidents in a certain type of traffic.

This analysis needs to be performed quickly, reducing the time between recognition and response. Artificial Intelligence will allow us to speed up the analysis of incidents and, thus, to improve the understanding of what is going on in the corporate network, to more precisely predict serious leaks, to faster detect incidents and faster answer them in order to diminish possible fraud and spoiling.

1.2. Increasing the use of Artificial Intelligence for security

Artificial intelligence and the learning machine significantly accelerate the response to threats, as it is stated by the analysts of Nemertes company. According to them, nowadays, Artificial Intelligence is a

³ https://www.hpe.com/emea_europe/en/home.html, accessed on 11.09.2019.



necessity, this having a serious market, created under the influence of a real need.

Specialists within Nemertes company⁴ made a study of global security and its results show that, as an average, it takes 39 days to detect and answer a cyber-attack, but some companies managed to reduce this amount of time to a few hours. The speed of the response depends directly on the level of automatization offered by artificial intelligence as well as the automatic learning of that company.

The average time for detecting an attack is one hour. In the most efficient companies that use artificial intelligence as well as automated learning, it takes less than 10 minutes to detect it. Regarding the average time for threat analysis, it is three hours. In the best companies, such an analysis lasts for a few minutes and, in the worst case, days or even weeks.

Financial service companies are in the spotlight. As their data is very valuable, they are usually one step ahead of everything in providing cyber security and they invest a lot in new technologies.

Regarding the applications of artificial intelligence automated learning, generally speaking, the figures are even higher. According to Vanson Bourne study, nowadays 80% of organizations use artificial intelligence to one purpose or another.

Garrigan Lyman Group introduces artificial intelligence and automated learning in order to approach a series of challenges connected to cyber-security, including the detection of a network and of the unusual activity of a user, as well as recognizing the newest phishing companies. Without the new technologies, it would be impossible to work normally, as the attackers have also resorted to artificial intelligence themselves, for a long time, automatizing their own activities, as Garrigan Lyman said.

Artificial intelligence and learning-machines give the upper hand to this company. The company is quite small, having only 125 employees, but it also has the capacity to introduce in the shortest amount of time the most recent technologies. At Garrigan Lyman, it is possible to operationalize useful innovations in only a few weeks. Especially the companies of fake alert information and Barracuda Networks use here security equipment and,

⁴ <https://www.cio.ru/articles/121117-Kak-iskusstvennyy-intellekt-mozhet-protivostoyat-kiberugrozam>, accessed on 12.09.2019.



just as Garrigan Lyman said, the most intelligent systems are those of retinal scanning.

Artificial intelligence helps systems adapt to the requirements of the company without implying the need for extensive formatting.

Another advantage of artificial intelligence is that it helps companies improve their products function of the clients' feedback.

*"Cyber security is like watching the neighborhood. If I notice something suspicious in our neighborhood, I will alert others"*⁵, said Chris Geysler, Technology Manager at Garrigan Lyman. Phishing methods or network attacks can be detected earlier in other time zones, allowing companies to prepare. Obviously, the service provider should be trustworthy.

The lack of confidence in innovation makes it difficult to pass from traditional processes to automatization based on artificial intelligence, as, besides knowing the peculiar features of your provider's activity, it will not overlap information regarding the manner in which artificial intelligence makes decisions. The principles set by experts in IT systems need to be clear so that to be trustworthy. Understanding the way in which the system functions, the client sends his/her feedback and wishes to get involved in improving the models of automated learning.

1.3. Artificial intelligence allows obtaining data before the attack of hackers

Artificial Intelligence helps increasing the amount of data we receive. When IT systems accumulate data gaps that are large enough, they become able to detect threat signals in the shortest time possible.

Due to learning machines. Companies do not only perform faster data processing, but they also correlate the events occurring in different moments in different locations. Some attacks can be repeated in a few weeks or months, on the Internet.

In order to successfully conduct the engine of a learning machine in a reasonable time, a lot of IT resources are needed.

⁵ <https://research-journal.org/economical/iskusstvennyj-intellekt/>, accessed on 12.09.2019.



According to cyber-security experts, when it comes to Artificial Intelligence, the providers of data protection solutions are way ahead of the hackers.

Therefore, companies rely on security measures that should remain efficient for a long period of time.

Yet, specialists in security need time to choose the best solutions as Artificial Intelligence also represents a hazard for companies, against which they need to defend themselves and that has nothing to do with piracy: marketing⁶.

IT specialists, after analyzing the phenomenon, identified several hardware or antivirus solutions and pretend that they are based on the newest versions of Artificial Intelligence regarding the protection of data in IT systems.

2. The hazard of Artificial Intelligence

Since the oldest times, man has devised things from the old science-fiction phantasies, from pocket calculators to self-driven cars, teleportation, virtual reality and, nowadays Artificial Intelligence.

Artificial Intelligence is nowadays a real perspective that companies in the whole world are focusing on.

“Artificial intelligence is a domain of science that focuses on the way in which hardware and software components of a computer can display an intelligent behavior”⁷.

Nowadays, there are many companies that work on Artificial Intelligence projects, including Microsoft, Facebook, Google and Minecraft. South Korea also has successful projects in Artificial Intelligence. Yet, we should not forget that there are other companies of great powers in the world (USA, Russian Federation, China etc.) that work secretly.

But why should Artificial Intelligence worry us? How dangerous is it really?

Nowadays, Artificial Intelligence, which used to exist only in human’s imagination, is quite real.

⁶ <https://www.journaldunet.com/solutions/expert/70239/cybersecurite---comment-l-intelligence-artificielle-peut-se-retourner-contre-vous.shtml>, accessed on 12.09.2019.

⁷ <https://rickscloud.com/how-dangerous-is-artificial-intelligence/>, accessed on 16.09.2019.



Lately, Artificial Intelligence has emerged as a highly interesting topic for many IT leaders, such as Stephen Hawking, Elon Musk, Bill Gates.

According to Bill Gates, “*artificial intelligence devices will be good at the beginning, but as they start to learn more and more from us and about us, they are going to get stronger and more intelligent than mankind*”⁸.

But which could be the risks incurred by Artificial Intelligence?

At present there are four risk classes incurred by Artificial Intelligence: *hostile malware risk; apathy risk; accident risk; unknown risk*⁹.

Hostile malware risk – the only possible scenarios through which Artificial Intelligence may be used for harmful purposes or deliberately programmed to be hostile (for instance, by a military or terrorist group).

Apathy risk – there is no clearly efficient risk of apathy coming from an Artificial Intelligence with a friendly super-objective, but it can be almost certainly found at an Artificial Intelligence without a friendly objective. Apathy in intelligence is simply dangerous because it does not take into account human safety just as people usually do.

Accident risk – if Artificial Intelligence works with incomplete data, it is possible that it makes wrong decisions, just as a person. These types of mistakes are hard to avoid, as it is impossible to know everything about the world, but these are less dangerous than all the four risks.

Unknown risk – the real danger of a well-designed Artificial Intelligence lies in its capacity to become reprogrammed or make its possible adjustments by itself. Any Artificial Intelligence is capable of improvement and is capable of eventually surpass human intelligence.

Even if there are a lot of opinions that characterize Artificial Intelligence as dangerous, we need to remember that these are only suppositions, not real facts.

People have always been distrustful regarding the new technologies and there even was a period of hesitation with respect to mobile phones.

⁸ <https://rickscloud.com/how-is-artificial-intelligence-changing-the-recruitment-practices>, accessed on 16.09.2019.

⁹ <https://rickscloud.com/3897-2/>, accessed on 16.09.2019.



Ultimately, the important thing is how we preserve and control Artificial Intelligence.

3. Implications of artificial intelligence in the military domain, upon security and defense

In the next decades, Artificial Intelligence is going to have major implications both upon the main domains of society, such as medical assistance, communications and transportation, as well as upon security and defense.

Thus, Artificial Intelligence, can be basically defined as “*systems that display an intelligent behavior and fulfill cognitive tasks analyzing their environment, taking measures and even learning from own experience*”¹⁰.

Nowadays, intelligent machines have become a reality in the modern world. The systems of Artificial Intelligence which exist nowadays can understand verbal orders, can discern images, can drive cars, can have very good results in games and, in a little while, there will be talks between a robot and a person and between two robots.

In the near future, “*artificial intelligence is going to take over more and more tasks and responsibilities of people that they are going to successfully fulfill, even better than humans*”¹¹.

Military forces are increasingly tempted to integrate the Artificial Intelligence technologies in order to guide or automatize their decisions. They are, at the same time, thought of as autonomous weapons that, in turn, are going to become possible targets in cyber-space.

In the military field, Artificial Intelligence is at the same time an opportunity and a hazard.

On the one hand, the lack of human supervision regarding the functioning of weapon systems with Artificial Intelligence, accompanied by the possibility that a system might be compromised could lead to actions and behaviors that would break the international laws of armed conflicts. It

¹⁰ Such a definition of AI is quoted in the European Commission’s Communication on “*Artificial Intelligence for Europe*”, COM (2018) 237 final, April 25, 2018.

¹¹ <https://gotech.world/inteligenta-artificiala-definitie-tipuri-de-ai-cum-invata-si-ce-aplicatii-are/>, accessed on 16.09.2019.



is quite unlikely that these systems respect human dignity. Their abusive use by non-state actors and their proliferation are also risks to consider.

On the other hand, the supporters of Artificial Intelligence are saying that such intelligence can effectively improve the military decision-making process.

Given the high degree of tension and emotion that usually surround conflicts, *“the Artificial Intelligence technologies might be implemented in order to improve logistic tasks, to improve the collection and interpretation of data, to ensure military and technological superiority, and to consolidate the possibility to combat reaction”*¹².

Regardless of the manner in which we view Artificial Intelligence, it is clear that *“its application in the conflict zone can raise questions regarding the future character of warfare and its strategic autonomy”*¹³.

3.1. Technical challenges, cultural and ethical aspects

In 2015 and also in 2017, a group of researchers, among whom Stephen Hawking as well as businessmen (such as Elon Musk) published an open letter, requiring the United Nations to stop the production of killer robots.

But what is it that worries specialists in Artificial Intelligence regarding these computers (killer robots)? The answer is the junction of technologies and robotics of learning machines, resulting in creating autonomous weapons capable of recognizing targets and making the decision to destroy them on their own.

Is it only science fiction? Not really. As this *“Terminator”* scenario is clearly a priority to some states, such as Russian Federation, China, United States of America, etc.

Russian Federation states that it is going to robotize at least of its armament by 2025.

¹² Michael C. Horowitz, *“The Promise and Peril of Military Applications Artificial Intelligence”*, Bulletin of the Atomic Scientists, April 23, 2018, https://thebulletin.org/landing_article/the-promise-and-peril-of-military-applications-of-artificial-intelligence/, accessed on 16.09.2019.

¹³ Aaron Mehta, *“AI makes Mattis question ‘fundamental’ beliefs about war”*, C4ISRNET, February 17, 2018, <https://www.c4isrnet.com/intel-geoint/2018/02/17/ai-makes-mattis-question-fundamental-beliefs-about-war/>, accessed on 16.09.2019.



“The army of the future is the army of robotized vehicles, ships, and aircraft”¹⁴.

Moreover, the famous armament producer, Kalashnikov, does not refrain from including several autonomous systems in its catalogue, due to using Artificial Intelligence that would be in the position to identify targets on the battlefield and make the decision to engage them without waiting for human intervention. Russian researchers’ work is displayed in a video that presents a humanoid robot (Feodor) that is gun-shooting at targets.

American researchers (SUA) also have a clip that presents prototypes of killer robots¹⁵.

China is another state interested in speeding up investments in robot technology for developing killer robots.

Could it be that World War III is going to be fought with killer robots only?

Here is a question that we cannot give a certain answer to, right now, but it may be true.

Yet, for the time being, in the absence of intelligent technologies, the fully autonomous weapons would probably not be operational on a battle-field.

“Having 100% autonomous weapons on the battle-field may result in a series of technical problems, as here we are dealing with some complex tasks”, explains Jean-Cristophe Noel, associated-researcher at the Center for Security Studies at French Institute of International Relationships (IFRI). The current solutions are limited applications... They are innovative and very useful, but still, limited. Moreover, man has not denied his part in the military; the cultural and ethical aspects of implementing autonomous weapons are not going to be erased overnight.

3.2. Artificial Intelligence – an aid to the operator identifying targets

The first Forum of Innovation Defense, organized at the end of November 2018, in Paris, offers a general picture of the most significant projects involving the French military and French businessmen.

¹⁴ https://www.defenseromania.ro/armata-viitorului-este-armata-vehiculelor-robotizate_597587.html, accessed on 17.09.2019.

¹⁵ https://www.ted.com/talks/pw_singer_on_robots_of_war?language=en, accessed on 17.09.2019.



They include the aerial drone program, designed by the naval group (prior DCNS) and Airbus, in order to endow the warships of French Navy. Derived from a civilian helicopter, these recon drones which will probably bear guns too are going to bear guns too, can be ordered starting with 2030.

The French project of aerial drones resembles the Franco-British project of combating underwater mines. It is only a matter of time until France and Great Britain and not only will be able to use this type of drones in order to detect and neutralize these threats. This project, led by Thales and BAE systems, is based especially on recon and classification technologies.

Another project of the French army is the autonomous target acquisition system, mounted on armored vehicles. Based on algorithmic chains capable of identifying in real time several types of targets through their thermic imprint and on a computer based on Kalray processors (designed in France), the system offers, for now, assistance to weapon operators.

French researcher in Artificial Intelligence, Jean-Cristophe Noel, quotes several representative cases for nowadays research.

The first American project - MAVEN. This consists in sorting and analyzing the images of drones in order to select the most important ones.

Artificial intelligence also offers aerial assistance on fighter aircraft. This means that the pilot is actually free to ignore certain tasks when he is oversaturated with information.

Finally, the applications capable to coordinate fire networks (for instance, to protect a ship under attack), as well as logistic ammunition flows.

“In my opinion, the main exercises that are going to be conducted will allow us to interpret as many sources of information as possible, to have maximal knowledge of the battlefield and recommend actions, taking into consideration, for instance, the doctrine of the respective army, the personality of opposing generals or data regarding the range of weapons used in the field”, said Jean-Cristophe Noel.

The most advanced projects of Artificial Intelligence that are being developed at present do not fully exclude the risks generated by the possible dramatic progress of IT technology.

According to the explanations offered by Jean-Cristophe Noel, if the current promises made by Artificial Intelligence are true and objectives are



reached in the domain of IT research, the impact will be quite remarkable and then we are going to witness a growth in automatization.

At the end of 2018, the Military Research Department in USA (DARPA) decided to allocate 2 billion \$ to a program of Artificial Intelligence called “*AI Next*”¹⁶, that aims at developing the next generations of technologies for Artificial Intelligence that are better adapted to decision-making and changing.

Some nations, led by the USA, are determined to go on increasing the autonomy of the machine and robotization and to reach a world in which the role of human is no longer essential in making decisions.

3.3. Breaking down Artificial Intelligence

The alarming increase in automatization is going to inevitably lead to a series of counter measures.

The IT systems hosting Artificial Intelligence, in turn, risk to become subject to cyber-attacks.

At the same time, IT systems are also subjected to a series of “*vulnerabilities specific to artificial intelligence: poisoning/shutting down; interference attacks; illusion attacks*”¹⁷.

For instance, making a test that involves Artificial Intelligence in which we will apply some sellotape on road signs, we will notice that we can trick algorithm of recognition of road signs by autonomous vehicles...

As the algorithms used in civilian situations are like those used in the military field, there is no doubt that autonomous (robotized) tanks, other autonomous armored vehicles or transportation modules are also going to be vulnerable to the neighboring technique.

3.4. Implications of Artificial Intelligence upon European Union security and defense

The European Union has already started to consider the “*possible implications of artificial intelligence in the domain of security and defense regarding autonomous weapons*”¹⁸.

¹⁶ <https://www.darpa.mil/work-with-us/ai-next-campaign>, accessed on 17.09.2019.

¹⁷ <https://versprite.com/blog/artificial-intelligence-security-vulnerabilities/>, accessed on 17.09.2019.



These reflections are necessary as there are frequent contradictory talks regarding conventional weapons, especially within the Convention regarding certain conventional weapons (CCW), as well as for the fact that *“USA, China and the Russian Federation are making progress with respect to the weapons and surveillance systems with the help of artificial intelligence”*¹⁹.

The European Union has started to admit the growing importance of Artificial Intelligence phenomenon, by signing a cooperation article among 25 European states in April 2018. More precisely, the preparing action regarding Preparatory Action on Defense Research (PADR) may include in the future elements of Artificial Intelligence.

The intention of European Commission is that of *“allocating 5% for Funding for European Defense (FED), for investments in the domain of research regarding artificial intelligence”*²⁰.

We also notice that the European Union signed in its Capability Development Plan (CDP), the importance of Artificial Intelligence as a future strategic factor in the security and protection of EU borders.

In this respect, *“on April 10th, 2018, 25 European states signed a declaration of cooperation in the domain of artificial intelligence”*²¹.

It is important that the perception on Artificial Intelligence be clearly understood regarding its meaning. This can be easily seen as a capacity in itself or as a technology considered as a strategic factor.

In addition, it is essential to underline the fact that *“most progress is not made in the defense and security domains, but in companied, through*

¹⁸ “European Parliament Resolution of 12 September on Autonomous Weapon Systems”, 2018/2752(RSP), Strasbourg, September 12, 2018, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0341+0+DOC+XML+V0//EN&language=EN>, accessed on 17.09.2019.

¹⁹ Samuel Bendett, “In AI, Russia is Hustling to Catch Up”, DefenseOne, April 4, 2018, <https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/>, accessed on 17.09.2019.

²⁰ European Commission, “EU Budget: Stepping Up the EU’s Role as a Security and Defence Provider”, June 13, 2018, http://europa.eu/rapid/press-release_IP-18-4121_en.htm, accessed on 17.09.2019.

²¹ European Commission, “Artificial Intelligence: Commission Outlines a European Approach to Boost Investment and Set Ethical Guidelines”, Brussels, April 25, 2018, http://europa.eu/rapid/press-release_IP-18-3362_en.htm, accessed on 18.09.2019.



*Amazon, Apple, Google, IBM and Microsoft, that invest billions of dollars in their Artificial Intelligence technologies and in the research and defense field*²².

European governments have understood the importance of innovation in Artificial Intelligence and a series of EU member states are developing national strategies for Artificial Intelligence and are investing governmental funds in this respect.

France has announced its intention to invest – until 2022 – in the domain of research for Artificial Intelligence, *“1.5 billion €, as part of the Country Innovation Plan*²³.

On July 18th, 2018, Germany announced that, within its national strategy regarding Artificial Intelligence, it is going to *“examine research and innovation, it will develop infrastructure and essential competencies*²⁴.

France and Germany are also going to cooperate in the domain of Artificial Intelligence and a series of other EU member states have developed or are currently developing national strategies regarding Artificial Intelligence (such as Estonia, Sweden and Finland).

*“The benefit in the domain of artificial intelligence would be between 6.5 - 12 trillion €, yearly, starting with 2025*²⁵. However, Artificial Intelligence also has its limitations and it takes a long time until we can say they have reached a certain maturity.

At present, Artificial Intelligence systems are capable of data reading, but there are limits regarding how far these systems can interpret this data. There is a disparity what is being read (reading) and reasoning in

²² *“Google leads in the race to dominate artificial intelligence”*, The Economist, December 7, 2017, <https://www.economist.com/business/2017/12/07/google-leads-in-the-race-to-dominate-artificial-intelligence>, accessed on 18.09.2019.

²³ Cédric Villani, *“Donner un sens à l’intelligence artificielle: pour une stratégie nationale et européenne”*, AI for Humanity, March, 2018, https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf, accessed on 18.09.2019.

²⁴ German Federal Government, *“Key points for a Federal Government Strategy on Artificial Intelligence”*, July 18, 2018, https://www.bmwi.de/Redaktion/EN/Downloads/E/key-points-for-federal-government-strategy-on-artificial-intelligence.pdf?__blob=publicationFile&v=4, accessed on 18.09.2019.

²⁵ <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>, accessed on 8.09.2019.



Artificial Intelligence. That is why, for the time being, people are playing an essential role in interpreting and reasoning with respect to data.

Continuing the investments in research in the domain of Artificial Intelligence is vital, especially if intelligent systems are going to be used efficiently and responsibly by the strong states of the world.

Success in the development of Artificial Intelligence in the domain of security and defense is going to largely depend on the governments that “*may invest sufficient capital and do have the necessary competences basis for artificial intelligence, research, security and defense, as well as robotics*”²⁶. Yet, most progress in Artificial Intelligence technologies is probably going to occur in the civilian area and an important role is going to be played by firms and research institutes.

4. Perspectives of using Artificial Intelligence in security

Detecting suspect user activity and network traffic are the most self-evident automated learning applications.

Nowadays, IT systems are increasingly capable of identifying unusual events of large data flows, solving standards of analysis tasks and sending notifications.

The next step is to use Artificial Intelligence in order to confront the most complex issues.

For instance, the level of cyber-risk for a company at a certain moment depends on a variety of factors, including the availability of unpaid systems, unprotected hubs, receiving phishing messages, level of viability of the password, amount of sensitive non-encrypted data, as well as whether the organization (company, etc.) is targeted by the intelligence services of another state.

The availability of a precise risk image would allow a more efficient use of resources and a more detailed set of performance indicators regarding security.

²⁶ Erik Brynjolfsson and Andrew McAfee, “*The Business of Artificial Intelligence*”, Harvard Business Review, July 18, 2017, <https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence>, accessed on 18.09.2019.



At present, relevant data is either not collected or not converted in significant information, as specified by Balbix, which predicts a risk of data leaking using Artificial Intelligence.

The IT specialists of the company have implemented 24 types of algorithms building up a “thermic map” of risks, taking into account all the characteristics of the client and allowing finding out why a certain “hot spot” is designated as such²⁷. At the same time, the service offers counselling regarding correcting the situation; if we are following what is going on, the red “hot” spot will be first yellow and then green. Furthermore, the system may ask questions such as “what should I do first?”, “which is my phishing risk” or “which is my risk of being a victim of hackers?”

In the future, Artificial Intelligence is going to help companies determine the kind of security technologies they should invest in.

“Most companies nowadays do not know how much time to spend on Cybersecurity”, said James Stanger, head of technology department at CompTIA.

At present, there is a large area for developing Artificial Intelligence. Artificial Intelligence is used in the domain of security, with certain limits.

The most exciting evolutions of Artificial Intelligence that mankind is going to benefit from are the following: *vocal recognition, virtual negotiator, decision-making, biometrics, natural linguistic processing, automated learning, language generation*²⁸.

It is possible to be talking soon about industry domains staying behind, such as is the case of car industry. There is only one branch of car industry that has particularly developed: that of automated driving of cars and less that of security networks protecting them.

Still, in other fields that make use of Artificial Intelligence, such as image recognition, discourse and weather forecast, there is a different situation.

²⁷ <https://www.cio.ru/articles/121117-Kak-iskusstvennyy-intellekt-mozhet-protivo-stoyat-kiberugrozam>, accessed on 19.09.2019.

²⁸ <https://rickscloud.com/artificial-intelligence-predictions/>, accessed on 20.09.2019.



“A hurricane is unable to change the laws of physics”, said McAfee, Director of Technology at CompTIA. The same happens in the world of cyber security.

Despite this situation, there is progress in the fight against cyber threats.

There is such a line of research with adverse generating networks, when two models of automated learning with opposing objectives function automatically. For instance, one is trying to detect one things and the other is trying to hide the same thing.

This could also be used in order to create conditioned enemy commands so as to find out the kinds of new threats which might occur.

Conclusions

In the next decades, Artificial Intelligence is bound to have major implications both on the main domains of society, such as medical assistance, communications and transports, as well as upon security and defense.

Artificial intelligence and automated learning are increasingly used in the domain of security and defense, especially in the field of cyber-security.

It is necessary that companies be one step ahead of hackers in developing IT security programs.

Artificial intelligence can rely on information about all kinds of threats in IT, known at world level, in order to detect any hacking attempt.

Artificial intelligence can also be used for implementing more secure authentication processes. Due to biometrics, it can be used for analyzing digital prints, the retina or vocal imprint.

In the real world, surveillance agencies and security services use Artificial Intelligence in order to foresee crimes before being committed.

In the military field, Artificial Intelligence is both an opportunity and a threat.

Military forces are more and more tempted to integrate Artificial Intelligence technologies in order to guide or automatize decisions. They are, at the same time, thought of as automated weapons which, in turn, are going to become possible targets in the cyber-space.



The army of the future is an army of robotized vehicles, ships and aircraft.

At present, there is no clear knowledge about how rapid the development of general Artificial Intelligence is, but there is a threat that a new level of Artificial Intelligence can be used by hackers as soon as it becomes available.

Certainly, the new evolutions in understanding knowledge, representation and manipulation, as well as automated learning, are going to contribute to increasing the level of security and defense of systems in the Artificial Intelligence domain.

Bibliography

1. Bendett, Samuel *"In AI, Russia is Hustling to Catch Up"*, DefenseOne, April 4, 2018, <https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/>.
2. Brynjolfsson, Erik and McAfee, Andrew *"The Business of Artificial Intelligence"*, Harvard Business Review, July 18, 2017, <https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence>.
3. Horowitz, Michael C. *"The Promise and Peril of Military Applications Artificial Intelligence"*, Bulletin of the Atomic Scientists, April 23, 2018, https://thebulletin.org/landing_article/the-promise-and-peril-of-military-applications-of-artificial-intelligence/.
4. Mehta, Aaron *"AI makes Mattis question 'fundamental' beliefs about war"*, C4ISRNET, February 17, 2018, <https://www.c4isrnet.com/intel-geoint/2018/02/17/ai-makes-mattis-question-fundamental-beliefs-about-war/>.
5. Villani, Cédric *"Donner un sens à l'intelligence artificielle: pour une stratégie nationale et européenne"*, AI for Humanity, March, 2018, https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf.
6. *** *"Google leads in the race to dominate artificial intelligence"*, The Economist, December 7, 2017.
7. *** European Commission, *"Artificial Intelligence: Commission*



Outlines a European Approach to Boost Investment and Set Ethical Guidelines, Brussels, April 25, 2018.

8. *** The European Commission's Communication on "Artificial Intelligence for Europe", COM(2018) 237 final, April 25, 2018.
9. *** European Commission, "EU Budget: Stepping Up the EU's Role as a Security and Defence Provider", June 13, 2018.
10. *** German Federal Government, "Key points for a Federal Government Strategy on Artificial Intelligence", July 18, 2018.
11. *** "European Parliament Resolution of 12 September on Autonomous Weapon Systems", 2018/2752(RSP), Strasbourg, September 12, 2018.
12. *** https://thebulletin.org/landing_article/the-promise-and-peril-of-military-applications-of-artificial-intelligence/.
13. *** <https://www.c4isrnet.com/intel-geoint/2018/02/17/ai-makes-mattis-question-fundamental-beliefs-about-war/>.
14. *** <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0341+0+DOC+XML+V0//EN&language=EN>.
15. *** <https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/>.
16. *** http://europa.eu/rapid/press-release_IP-18-4121_en.htm.
17. *** http://europa.eu/rapid/press-release_IP-18-3362_en.htm.
18. *** <https://www.economist.com/business/2017/12/07/google-leads-in-the-race-to-dominate-artificial-intelligence>.
19. *** https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf.
20. *** https://www.bmwi.de/Redaktion/EN/Downloads/E/key-points-for-federal-government-strategy-on-artificial-intelligence.pdf?__blob=publicationFile&v=4.
21. *** <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>.
22. *** <https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence>.



23. *** <https://www.cio.ru/articles/121117-Kak-iskusstvennyy-intellekt-mozhet-protivostoyat-kiberugrozam>.
24. *** <https://rickscloud.com/artificial-intelligence-predictions/>.
25. *** https://www.hpe.com/emea_europe/en/home.html.
26. *** <https://www.cio.ru/articles/121117-Kak-iskusstvennyy-intellekt-mozhet-protivostoyat-kiberugrozam>.
27. *** <https://research-journal.org/economical/iskusstvennyj-intellekt/>.
28. *** <https://www.journaldunet.com/solutions/expert/70239/cybersecurite---comment-l-intelligence-artificielle-peut-se-retourner-contre-vous.shtml>.
29. *** <https://rickscloud.com/how-dangerous-is-artificial-intelligence/>.
30. *** <https://rickscloud.com/how-is-artificial-intelligence-changing-the-recruitment-practices/>.
31. *** <https://rickscloud.com/3897-2/>.
32. *** <https://gotech.world/inteligenta-artificiala-definitie-tipuri-de-ai-cum-invata-si-ce-aplicatii-are/>.
33. *** https://www.ted.com/talks/pw_singer_on_robots_of_war?language=en.
34. *** <https://www.darpa.mil/work-with-us/ai-next-campaign>.
35. *** https://www.defenseromania.ro/armata-viitorului-este-armata-vehiculelor-robotizate_597587.html.
36. *** <https://versprite.com/blog/artificial-intelligence-security-vulnerabilities/>.



PARTICULARITIES OF THE ROMANIAN MIGRATION IN THE POST COLD WAR PERIOD

PhD student Alina ARDELEANU

National School of Political and Administrative Studies,

E-mail: alina.ardeleanu7@yahoo.com

Abstract: *Migration represents one of the issues that Romania, through its political environment, has fully acknowledged and which it constantly strives to improve. After the disintegration of the USSR, the migration phenomenon began to gain scope compared to the communist period. The exponential increase in the number of migrants was remarked after Romania's accession to the European Union. Over the past 30 years, the role of diasporas has become a strategic one in international affairs. This is an aspect which Romania will have to meditate and capitalize on. Taking into consideration that the Romanian diaspora is in the top 5 worldwide, the Romanian state cannot ignore it and can only collaborate with it.*

The approaches taken by our country, concerning the strengthening relations with its diaspora are still in progress.

Keywords: *migration, diaspora, Schengen, migrants, European Union.*

General aspects regarding the migration phenomenon

Migration seems to be a current concern in a lot of states forming the great network of international relations. However, the phenomenon has been quite active since the oldest times. Depending on the age, different historic circumstances and the evolution of concepts in social sciences, migration has raised the interest of many researchers in various fields such as: historians, economists, sociologist, anthropologists, geographers, experts in international relations, in security studies, in political or juridical sciences. All the researchers interested in this topic have tried to create an adequate theoretical framework, yet, without making significant progress.

Even though the literature in the field comprises a series of migration theories that any research, any scientific endeavor needs to take into account, we are still far from the theoretical frame we would like to have. As there are so many theories regarding this phenomenon, it is very



difficult for us to promote a common and complete vision regarding the theoretical approach of this concept. The majority of experts and researchers on migration issues have concluded that the inconsistency of the current theories, as well as their ample nature make it impossible for us to relate to one single theoretical, expository model.¹ Therefore, the common vision upon migration remains an aim envisaged not only by researchers, but also by political factors.

The Romanian literature in the field is quite scarce on this topic and more often than not, it recycles the same information.

Migration can be defined in terms of mobility of population, referring to the permanent or temporary moving house of a person or a group of people, both from an administrative-territorial unit to another, and outside the country².

The causes and effects of Romanian migration

We can state that Romanian migration is quite recent and, despite this fact, it has a growing influence on the Romanian society, becoming a fundamental issue that raised the interest of researchers, employers, politicians, as well as regular Romanians. The year 1989 was characterized, among other things, by the falling of border boundaries, allowing Romanians to go to other states, without jeopardizing the security of family members left behind. The communist period was characterized by a low migratory movement, as “severe control was enforced upon the international movement of population, materialized by restricting access to passports and blaming those who openly stated their intention to leave the country and who, on various routes, legal or not, managed to emigrate and settle down in another country”³.

In 1990, one of the first measures taken by the transient government in Romania was opening up the passport regime. The right to have a

¹ Cristina Haruța, *Migrația ca fenomen social: perspective și abordări teoretice transdisciplinare*, în *Revista transilvană de Științe Administrative*, 2 (43), 2018, p. 34.

² Ciprian Iftimoaei, Ionuț Cristian Baci, *Analiza statistică a migrației externe după aderarea României la Uniunea Europeană*, în *Romanian Statistical Review- Supplement* Nr. 2, 2018, p. 169.

³ Alexandra Sarcinschi, *Migrația ca problemă de securitate. Studiu de caz: România*, Editura Universității Naționale de Apărare „Carol I”, București, 2014, p. 38.



passport and get out of the country depended only the financial means, as entering several Western countries was also unrestricted through a visa regime. Thus, many people engaged in various types of international mobilities. A lot of them used this freedom to simply travel, while others combined travel with the “luggage trade” (Diminescu, 2009, p. 46). Yet, a significant number of Romanian citizens tried to reproduce the emigration model that had functioned in the communist era: by resorting to the right to political asylum, they tried to obtain a legal status and, in time, legal residence and complete emigration to the West⁴.

Both during the communist era and during the post-Cold War period, the destinations preferred by Romanians were in the West. The reformation of Romania, from the economic point of view, led to cutting out 3.5 million employment opportunities, which made Romanians go abroad, their favorite destinations being Italy, Germany, Spain, France, Great Britain, Israel, Hungary⁵. The migration-oriented behavior became almost specific to the states crossing a period of economic, political, or social transition. Even though Romania became a state both of origin and destination of international migration, the predominant trend makes it a clearly observable emigration country.⁶

The issue of Romanian migration has become imperative and current estimates seem to leave us no place to react. Statistically speaking, over one third of the whole number of Romanian households have a member gone abroad, or even more than that⁷.

It is completely wrong to assume that Romanians choose to settle down abroad only for financial reasons. Although some of the Romanian migrants might have decent income in our country too, they choose to leave because they feel they resonate better with a certain type of culture, with the specific aspects of a certain country. For instance, we have got Romanian

⁴ Horvath István, cap. 7. *Migrația internațională a cetățenilor români după 1989*, p.201, www.scribd.ro.

⁵ Constantin Anghelache, Georgiana Niță, *Migrația- factori determinanți și modele economice*, în *Romanian Statistical Review*, Supplement Nr. 5, 2018.

⁶ Bogdan Alexandru Suditu (coord.), *Studii de Strategie și Politici (SPOS) 2012. Studiul nr. 1. Perspectivele politicii de migrație în contextul demografic actual din România*, Institutul European din România, București, 2013, p. 153.

⁷ Petronela Daniela Feraru, *Migrație și dezvoltare*, Editura Lumen, Iași, 2011, pp. 2-3.



doctors who choose to work in Western hospitals not only for solely economic reasons, but also for the superior working conditions there. Other Romanians choose to settle down in states where not only the economic situation is good, but also where there is political and social stability.

In order to somewhat establish the causes of Romanian migration from exactly those who have made this step, the Ministry for Romanians Everywhere (in Romanian, Ministerul pentru Români de Pretutindeni) made up a survey entitled “MRP Survey addressed to Romanian Everywhere”⁸. The experts of the ministry request the following data from the Romanians abroad: the states where they live, the towns/villages in the respective state, the counties of origin from Romania, the gender, the age group, the domain in which they work, the reason/reasons they chose to settle abroad, the actions taken by the host country to integrate Romanians, the main factors through which Romanian identity is consolidated in the residence state and the sources of information they consult in order to find out about the situation within the country. Among other things, the Romanians in diaspora are asked about the potential problems they might have been forced to face regarding the right to work or the right to stay there. Moreover, the survey attempts to find out the measure in which our citizens wish to return to the country in a reasonable period of time.

When all the answers are analyzed, the result will be a solid foundation which the habilitated institutions might start from, formulating efficient public policies that might not only determine Romanian migrants to return home, but also determine them to cooperate with the Romanian state, at least those of them who have made a final decision regarding permanent residence on other states’ territories.

A report recently made by OECD shows the fact that Romanian diaspora is in top 5 in the world (in relation to the whole number of population). Given this situation, especially as Romania is far from going through a climate of an armed confrontation, the Romanian state cannot ignore its diaspora, being necessary to constantly find concrete methods and ways to establish better cooperation with it.

⁸ *** The questionnaire can be consulted at the following web address:
<http://www.mprp.gov.ro/web/chestionar-mrp-adresat-romanilor-de-pretutindeni/>.



One of the most significant causes that contributed to the sudden and alarming increase in the number of Romanian migrants was our country's adhering to the European Union. Since 2002, we have benefitted from a visa waver program in the Schengen area for up to 90 days. After Romania's accession to the European Union, Romanian citizens could benefit from the provisions of article 45 in the Treaty on the Functioning of European Union as follows: "the free movement of workers is guaranteed within the Union"⁹.

According to the second paragraph of the same article, "free movement implies eliminating any discrimination on grounds of citizenship among the workers of member states, regarding positions, remuneration and the other work conditions"¹⁰.

We need to take also take into account the fact that the migration of highly qualified individuals is influenced by their studies and expertise which generate different pull factors and push factors. For instance, the reasons for emigration of a researcher may be personal aspirations and scientific curiosity; those of a manager may be the reflection of the employer's priorities; for academics and students, the reasons might be the attraction towards the countries in which the national systems of innovation / universities are extremely developed and in which "scientific open-mindedness" is a priority; while for scientists and engineers, the pull factors could be the countries / companies that have the reputation of offering jobs in the domains of innovation and new technologies (Mahroum, 2000). Moreover, in case of all highly qualified workers, the pull factors outrank the push factors¹¹.

It is not only in Romania, but also in many other states, that migration is regarded as a negative externalization. This vision does not target only the unqualified migrants, but also the highly qualified ones. Our country faces both situations. Even if migration is temporary and those who

⁹ **Tratatul privind funcționarea Uniunii Europene (versiunea consolidată)*, available at https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_2&format=PDF, accessed on 24 octombrie 2019.

¹⁰ *Ibidem*.

¹¹ *****Emigrația forței de muncă înalt calificate din România. O analiză a domeniilor cercetare – dezvoltare, medicină și tehnologia informației și a comunicațiilor. Raport de cercetare*, www.emit.cdcdi.ro.



leave the country choose to come back after a certain period of time, then Romania might create the necessary frame for being able to benefit from their expertise gained / enriched. A priority for the Romanian state would be identifying the possibilities through which we might capitalize on the experience of Romanians coming back to the country, leading to the transformation of what seemed to be a loss past retrieval or hardly retrievable into a potential gain. A possible error would be adopting an over-simplified approach of this issue, Romania having to demonstrate that it understood why its citizens had chosen to settle down in other states. Moreover, equal opportunity should be guaranteed regarding the chances of assertion.

There are two essential directions that result from this situation and that the Romanian state has to keep in mind: offer Romanians sufficient reasons to stop them from leaving or to determine them to come back, respectively, organize them in diasporas and use them in order to develop the society they originate from.

The return of qualified people is not a fact which is simple to control or influence. In most cases, the affective connections between those who leave and those who stay in the country are not so strong as to make most of the Romanians in diaspora to return to the country at a certain moment. Supposing that they had left for economic reasons, it is difficult to believe that they will return before having the certainty that they will be able to ensure in the country the financial balance similar to that in the host state. Even if economic problems were to disappear, we could not be sure that the Romanians settled abroad would return to the country. As we have mentioned above, the developed countries are not considered dream destinations by most migrants only for financial reasons, but also due to the level of civilization / education they might find there or the cultural attraction they might feel when relating to a certain state.

Four years ago, Romanian Presidency took on the role of supporter of Romanian people's rights both outside and inside the borders, showing the necessity to capitalize the strategic potential that Romanian diaspora might benefit from, which may acquire the role of connection with other states. A first step was creating within the Romanian Presidency a new department called the Department for Relation with the Romanians Outside the Borders.



Also, a few concrete steps were taken for improving the relationship of cooperation between the Romanian state and its diaspora by the Government. In 2017, the Ministry for Romanians Everywhere was set up. The new ministry took over two departments from the structure of the Ministry of External Affairs. These were the Department of Policies for the relationship with Romanians Everywhere and the “Eudoxiu Hurmuzachi” Institute for the Romanians Everywhere¹².

Conclusions

The migration phenomenon will not be able to be stopped by a democratic Romania, regardless of the measures that might be taken therefore Romanian Government and the other responsible authorities should work on two levels: supporting the Romanian migrants to return to the country and consolidating the relations of the Romanian state with its diaspora which, in certain contexts, may become a solid pillar in the relations that Romania may have with other states. The functions of Romanian diaspora (consolidating the spiritual culture of the people of origin; preserving the ethnic culture; defending social rights; economic and political functions) need to be kept in mind and taken advantage of by our country.

The members of the diaspora will cultivate traditions and customs from the country of origin, and they will keep intact our national language. For instance, in states where there are large communities of Romanians, there are a lot of its members who have the habit of getting together and spending time together on different special occasions. This function is hardly usable where there are small communities of Romanians, as they are assimilated by the population of the state where they live. Romanian economy is to a certain extent dependent on the money sent by the diaspora to the country. Even if the respective sums of money are not taxed, they are directly integrated in the consumption economy. The political function of Romanian diaspora is quite little valorized, which is going to have to

¹² **S-a înființat Ministerul pentru Românii de Pretutindeni, into the <http://www.mprp.gov.ro/web/s-a-infiintat-Ministerul-pentru-romanii-de-pretutindeni-2/>, accessed on 06. 09. 2019.



become a priority, but only after a good analysis of the necessities and potential of Romanian migrants.

Bibliography

1. *** *Tratatul privind funcționarea Uniunii Europene (versiunea consolidată).*
2. *** *S-a înființat Ministerul pentru Românii de Pretutindeni*, into the <http://www.mprp.gov.ro/web/s-a-infiintat-ministerul-pentru-romanii-de-pretutindeni-2/>.
3. *** <http://www.mprp.gov.ro/web/chestionar-mrp-adresat-romanilor-de-pretutindeni/>.
4. *** *Emigrația forței de muncă înalt calificate din România. O analiză a domeniilor cercetare – dezvoltare, medicină și tehnologia informației și a comunicațiilor. Raport de cercetare*, www.emit.cdcdi.ro.
5. Anghelache, Constantin; Niță, Georgiana *Migrația- factori determinanți și modele economice*, în *Romanian Statistical Review*, Supplement Nr. 5, 2018.
6. Feraru, Petronela Daniela *Migrație și dezvoltare*, Editura Lumen, Iași, 2011.
7. Haruța, Cristina *Migrația ca fenomen social: perspective și abordări teoretice transdisciplinare*, în *Revista transilvană de Științe Administrative*, 2 (43), 2018.
8. Iftimoaei, Ciprian; Baci, Ionuț Cristian *Analiza statistică a migrației externe după aderarea României la Uniunea Europeană*, în *Romanian Statistical Review- Supplement Nr. 2*, 2018.
9. István, Horváth *cap. 7. Migrația internațională a cetățenilor români după 1989*, p.201, www.scribd.ro.
10. Sarcinschi, Alexandra *Migrația ca problemă de securitate. Studiu de caz: România*, Editura Universității Naționale de Apărare „Carol I”, București, 2014.
11. Suditu, Bogdan Alexandru (coord.) *Studii de Strategie și Politici (SPOS) 2012. Studiul nr. 1. Perspectivele politicii de migrație în contextul demografic actual din România*, Institutul European din România, București, 2013.

