REVISTA ACADEMIEI DE ȘTIINȚE ALE SECURITĂȚII NAȚIONALE ANUL V, 2020   NR.1 (08)

RASSN

Revista Academiei de Științe ale Securității Naționale

NR. 1/2020

ȘTIINȚE MILITARE

INFORMAȚII ȘI SECURITATE NAȚIONALĂ

ORDINE PUBLICĂ

Journal of The Academy of National Security Sciences

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

CONTENTS

EDITORIAL

NEW TIMES / NEW ACTORS (I)

Our planet is actually a *„global village",* with economies and interests that are increasingly inter-connected. The wars in different parts of the world, especially in the Middle East, the internal turmoil, the fight against criminality, the border control and pandemics are all situations which are hard to control, necessitating continuous and careful evaluations from institutions that play a part in ensuring national defense and security.

The armed forces, or the army as the generic term is usually used, has been and is going to continue to be involved in all these issues (crises). National defense and security are nowadays approached from a systemic perspective. Security is a multidimensional concept (political, diplomatic, military, economic, scientific, information, cultural, social and so on), which is omnipresent and omnidirectional, each domain taking measures to promote the interests specific to each one.

We can say that the policy of national security and defense, promoted by the political factor, has to take into account the fact that the vital connections among the sectors (dimensions) of national security and defense actually determine their optimal functioning. Yet, this has to be well-understood by all decision-makers and not to be recalled only in limit situations (as it happens nowadays). The balance of the system and its optimal functioning is theoretically based on and practically ensured by measures for promoting fundamental national interests and defending them against any aggressions, threats, risks, and vulnerabilities.

The present trend perceived by specialists tends towards a new international system, another settlement of states in the world power structure, which is vital to the physiognomy and future of mankind. The correct understanding and definition of risks, threats, and vulnerabilities generate extended national security.

Global threats did not become smaller, they only changed. The threat of a war was replaced, at least in Europe, with a lot of risk factors, whose significance varies from one region to another. Yet, instability has spread. Conflicts have become increasingly explosive, manifesting as a large array of social, ethnic, religious, economic crises and even inter- and intra-state competition, now in addition to global pandemic.

As conflicts and crises fall under the categories mentioned above, military planners need to adjust and recalibrate military structures accordingly and, at the same time, they have to find tactics and strategies meant to oppose and counter the new range of threats. Everybody is aware that, at present, there is a considerable extension of the concept so as to express the interaction of political, economic, military, technological, cultural, juridical factors.

Building the destiny of Romania, Europe, and the world generally speaking is going to depend on the aptitudes and capacities of the current and future power poles, with maximal efficiency in global issues, as well as on the capacity of harmonizing interests in different areas. We also consider that eliminating /diminishing the role of a power pole is bound to crush the entire architecture of security, irrespective of how favorable or generous there might be the geopolitical, geostrategic and geoeconomic scenario they were designed for.

Geopolitical analyses at global level show the fact that, at periodical intervals (no longer than half a century), there has been a process of rethinking and redefining international relations. The main results should be reducing the probabilities of confrontation, achieving a climate of partnership and collaboration, all of them with the goal of shaping the

architecture of security. Yet, the constant issue at all times has been maintaining risks and threats to states, including Romania. These risk factors which are non-military, asymmetric, asynchronous, unconventional represent a rather significant potential danger to global, regional, zonal and local security.

As a result, contemporary reality requires political factors to permanently have available forces and means that are prepared, professional, adapted to current realities in order to manage crises. *Armed Forces are neither better nor worse than the political decision makers who set their tasks and establish their missions.*

What we really need is a long-term political will and vision beside national cohesion and pragmatism. We need to be able to timely predict crises of any kind, to have experts and professional forces specialized in dealing with internal crises in order to ensure extended security and national defense. Starting from this contemporary reality, we have to underline the necessity of becoming fully aware of the crisis phenomena as well as of the actions which might be conducted in order to manage and combat them.

Brigadier General (ret.) Professor Gheorghe Toma, PhD

CORONACRIZA – PROVOCĂRI PENTRU VIITOR!

CORONACRISIS – CHALLENGES FOR THE FUTURE

Major General (ret.) Professor Gabriel-Florin MOISESCU, PhD
Tenured member of the Academy of National Security Sciences,
E-mail: moisescu.gbrl@gmail.com

Rezumat: Pandemia de coronavirus este considerată de către specialişti un eveniment de tip Lebăda Albă şi/sau Rinocerul Gri. Prin impactul său major, acesta a „paralizat" autorităţile statelor din întreaga lume o perioadă de timp, fapt ce a determinat ca acestea să acţioneze „fiecare pentru el".

Ulterior, au fost puse în mişcare mecanismele de colaborare şi cooperare ale Uniunii Europene, Alianţei Nord Atlantice, parteneriatelor etc.

Funcţionarea autonomă a statelor în perioada aceasta este propunerea noastră pentru ca nici un stat, în situaţii de criză, să nu devină o povară pentru celelalte.

Cuvinte cheie: Pandemie, tip de eveniment, autorităţile statului, perioada, funcţionare autonomă, industrie naţională de securitate.

Abstract: Coronavirus pandemic is considered by specialists a White Swan and/or a Gray Rhino. Through its major impact, it has „paralyzed" the authorities of all the states in the world for a certain period which created the need that each of these should act „on its own and for itself".

Subsequently, collaboration and cooperation mechanisms started to be put into motion, such as those of the European Union, the North Atlantic Treaty Organization, partnerships etc.

The autonomous functioning of states in this period is our proposition so as no state, in crisis circumstances, might become a burden to the others.

Keywords: pandemic, type of event, state authorities, period, autonomous functioning, national security industry.

Nowadays, when you get into contact with the real world, you might have the feeling that you have gone back in time. It seems that the world has stood still. Technology is the only factor that reminds us that we are in the 21st century. Otherwise, we might feel like some actors playing in a science-fiction movie: people with protection masks and gloves, keeping distance from each other while trying to purchase goods of strict necessity and medicine, police, gendarmerie, and military teams at all crossroads,

ambulances etc. There is a certain tension in the air, impossible not to feel, certainly caused by this killer virus, COVID-19, which appeared out of nowhere and is probably going to disappear the same way.

On Venice canals, once overcrowded with gondolas packed with tourists, we can see dolphins playing happily in the water which is cleaner and cleaner, and swans seem to be "breathing better" relieved that "finally our habitat is quiet".

So, nature is "breathing" and carrying on with its life, yet warning us that there should be some balance between it and human beings and that an absolute priority of mankind should be giving the environment its well-deserved importance.

So this is the world we are living in today!

What kind of events should include the pandemic? Why did we get here? Where are we now? How could we get over these times? What should we do in order for something like this not to happen again? These are all questions whose answers we are going to try to find in the current scientific endeavor.

Coronavirus pandemic was initially considered a Black Swan type of event which, according to the author of the theory, Nassim Nicholas Taleb, has three characteristic features[1]: an isolated case having a major impact and retrospective predictability (,,…, human nature made us come up with explanations after its occurrence, after it happened, making it explainable and predictable"[2]).

Examples[3] of Black Swans are the following: Hitler's rise to power and 2nd World War, the quick dismantling of the Soviet bloc, the spread of the internet, the financial crisis of 1987, the terrorist attack of September 11th, 2001.

---

[1] Nassim Nicholas Taleb, *LEBĂDA NEAGRĂ*, impactul foarte puţin probabil, Editura Curtea Veche, Bucureşti, 2009, pp. 14-15.
[2] *Ibidem*, p.14.
[3] *Ibidem.*

Yet, the actual author of the theory denied the fact that the coronavirus pandemic was a Black Swan kind of event and is now saying that it was a White Swan[4] as it might have been prevented[5].

From the point of view of American analyst Michele Wueker, the best suited metaphor for this kind of event would be the Gray Rhino, corresponding to a threat which is quite likely to occur and with serious impact, which has however been neglected[6].

Unlike Taleb, Nouriel Roubini, the one who predicted the crisis in 2008, does not consider financial crises as Black Swans, but associates them with hurricanes, being the predictable outcome of a sum of economic and financial vulnerabilities and political errors. According to him, the pandemic may throw economy into a crisis that would be bigger than the one in 1929-1933[7].

Given all the arguments presented above, we consider that the pandemic, as type of event, may be associated with both the metaphor of the White Swan and with that of the Gray Rhino, as they have the characteristics identified by their authors.

Moreover, we are in agreement with analyst Michele Wueker, who considered that doing something in order to fix the things we see in front of ourselves („paying attention to the Gray Rhino") would mean to make better use of the time available as compared to trying to find the Black Swans[8].

Why has it come to this?

---

[4] The White Swan is a rare, unpredictable event that has positive effects; the Gray Swan is an event whose effects can be predicted up to a certain point, but whose occurrence is unlikely, according to *[https://descopera.org >teoria-l...],* accessed on 02.04.2020.

[5] Nassim Nicholas Taleb, interview for Bloomberg, according to *[https://romania.europalibera.org>d...],* accessed on 02.04.2020.

[6] The Gray Rhino is a massive, two-ton animal, with the horn oriented towards you, treading the earth and preparing for an attack and – most importantly – offering you the chance to act (Michele Wueker in the article for Washington Post. The metaphor was used for the financial crisis in Greece in 2012).

[7] *Ibidem.*

[8] *[https://revistasinteza.ro>profe....],* accessed on 02.04.2020.

First of all, due to a profound connectivity which, according to the insufficient attention paid to the environment, represent another issue that today's world is confronting[9].

Then, the confidence syndrome, in the sense that we believe that this cannot happen to me/us, an attitude which, in time, led to a lack of timely involvement and of responsibility from governments all over the world which, in turn, led to postponing making decisions regarding limiting the spreading of and even stopping the pandemic[10].

At the same time, in the initial stage we did not take into account its economic effects or the fact that it is impossible to separate combatting the pandemic from economic problems, as they are hardly two parallel universes. [11]

Also, it is shown that governments, companies and corporations have no excuse for not having prepared for such an event.[12]

According to specialists[13], information has existed since 2019, when epidemiologists and health experts warned that the world was „ripe" for the following pandemics and global traffic, climate change and resistance to antibiotics have made mankind more vulnerable.

In the same year, National Intelligence Service in the USA issued a global warning referring to the fact that the USA and the whole world are going to prove vulnerable to the next pandemic or a contagious disease, with serious effects upon world economy and international resources.

In the same respect, some analysts[14] consider that the pandemic might have been prevented if, on January 26th, when necessity to stop it at all costs from spreading was clearly stated, there would have been extremely rapid reactions.

Nobody can afford to look for someone to blame during these times, but we believe that the mistakes made in combatting the pandemic should

---

[9] *[https://romania.europalibera.org>d…], accessed on 02.04.2020.*

[10] *[https://romania.europalibera.org>d…], accessed on 02.04.2020.*

[11] *[https://revistasinteza.ro>profe....], accessed on 02.04.2020.*

[12] *Ibidem.*

[13] Michele Wueker, *[https://revistasinteza.ro>profe....], accessed on 02.04.2020.*

[14] Nassim Nicholas Taleb, *[https://romania.europalibera.org>d…], accessed on 02.04.2020.*

be taken care of and we, humans, need to join hands and act together so as to defeat this insidious and lethal virus.

Where are we now?

Now we are in the situation[15] in which almost half of the planet is isolated at home, with a number of confirmed cases approaching one million and a number of deaths of 40.000, half of which only in Italy and Spain. We are dealing with the worst humanitarian crisis after 2nd World War that is probably going to result in a recession impossible to compare to anything from the recent past[16].

The European Union, „inactive" for a while, just like the other global and regional organizations, is preparing a common recovery plan[17] which has unfortunately produced an acute division between the Southern and the Northern states (Italy and Spain proposed sharing the debt instruments – „corona-bonds" – but Germany, together other states from the North, rejected this idea of assuming the debts caused by the pandemic).

NATO also gathered together (also late from our point of view, and also after some time) at first through a secure video conference (02.04.2020) and, through the voice of its Secretary General, it asserted its support – through its armed forces – for nations in their struggle against the coronavirus crisis (thus answering Italy and Spain's requests by facilitating Spain's receiving of medical supplies from Czech Republic and Turkey's sending a plane with medical materials and equipment to Spain and Italy)[18].

At the same time, through the voice of one of its high officials[19], NATO declared the current crisis a threat to global security, a security risk that is different in nature from others, but no less dangerous and insidious, as well as the fact that the mobilization of security resources, especially

---

[15] Secretarul general al Organizaţiei Naţiunilor Unite, Antonio Guterres, conform *[http://romania. europalibera.org],* accesat la 02.04.2020.
[16] United Nations Organization Secretary General, Antonio Guterres, according to *[http://romania. europalibera.org],* accessed on 02.04.2020.
[17] United Nations Organization Secretary General, Antonio Guterres, according to *[http://romania. europalibera.org],* accesed on 02.04.2020.
[18] *[evz.ro],* accessed on 02.04.2020.
[19] N.A. Mircea Geoană, NATO Deputy Secretary General; *[www.rador.ro > N.A.T.O.],* accessed on 02.04.2020.

economic ones, are a lesson with respect to future investment in the security sector.[20]

As far as our country is concerned, while the Chinese authorities were fighting the virus, our politicians were fighting for power, probably thinking according to the syndrome mentioned above, that the virus was some place far away and nothing can happen to us.

Afterwards, when World Health Organization (WHO) declared the pandemic, we started to react (also after some time), the idea of holding anticipated elections was given up and a legal government with full rights was put in place.

While we are writing these lines, Romania is still in State of Emergency, by a Decree signed by Romanian President on 16.03.2020, following the Decision of Supreme Council for Country Defense (CSAT) no.30/2020 and the declaration of pandemic by WHO on 11.03.2020[21], and has entered the 4th alert scenario (with over 2,000 cases of infected people).

No country in the world was prepared to deal with this virus from the beginning; specialists had to learn little by little, adjusting permanently to its evolution and mutations.

The fact that decision-making was postponed by the authorities, the high speed of virus propagation, the major impact, the unpredictability of evolution made the largest part of health systems, irrespective of the level of development of the respective state, to be taken by surprise by having to deal with this kind of event on medium and long term, as there was an acute lack of protection equipment (gloves, masks, overalls, goggles), medical devices and equipment (for testing, ventilators etc.), tests, medicine, beds, specialized transportation means, specialized human resource etc.

Why did this happen?

Because, from our point of view, in almost the entire world, profit chasing started to be considered much more important than solving social issues, reason for which we need to embrace the opinion of a reputed analyst who said that the „origin of this crisis is a huge dysfunctionality of

---

[20] *Ibidem.*
[21] *[https://, presidency.ro> media],* accessed on 30.03.2020.

the market and neo-liberal policies which intensified socio-economic issues"[22].

This is how the result was that Germany could not help Greece, but Cuba helps European countries[23].

How can we go over these times?

First of all, our opinion is that state authorities need to have single leadership (in our country, even though there are, according to the law, such bodies – National Committee for Special Emergency Situations, the Strategic Communication Group under its command, the County Committees for Emergency situations etc. – their activity is hindered by the excessive involvement of local authorities).

Secondly, there should be a „single voice" (we believe that at times like these, politicking should be banned from all speeches and politicians should respect their promises and commitments they had assumed with respect to the country and its citizens).

Thirdly, we should be able to protect our people in the „first line", the medical staff, and provide for them whatever they need.

At the same time, authorities need to take economic and fiscal-budgetary measures, especially among employees, in order to ensure continuity of functioning in economy and preserving employment opportunities and jobs that are so necessary for a rapid starting over in the post-pandemic period.

Similarly, we need to respect the norms transmitted by authorities and the adequate preventive measures; yet, this should be valid for everyone, not only for some of us, as foolishness is universal and against it "the gods themselves" fight in vain[24].

---

[22] Naom Chomsky, an interview called „*Coronavirus – what is at stake*" given to Srećko Horvat at DiEM25-TV in Arizona, on 28th March 2020; according to *[https://internal. diem25.org>events],* accessed on 03.04.2020; *[m.youtube. com],* accessed on 03.04.2020.
[23] Naom Chomsky, an interview called „*Coronavirus – what is at stake*" given to Srećko Horvat at DiEM25-TV in Arizona, *op.cit.*
[24] N.A. This was inspired by Isaac Asimov's novel, *Zeii înşişi*, Editura Teora, Bucureşti 1993. The author dedicates this book to mankind „*and to the hope that the fight against foolishness may be won someday*" (p. 2). The contents of the work are divided into three parts: part one – *against foolishness*…; part two – *the gods themselves* …; part three: *the fight in vain*.

Finally, last but not least, it is extremely important that the appointed forces permanently watch so that law is observed.

A corollary of the arguments presented above could be comprised in four words: responsibility, involvement, solidarity and respect.

What should we do so that this may not happen again?

We need to be aware of the fact that we are living in an international political system which is an anarchy whose main feature is sovereignty, a structural state favoring competitive relations[25], in a world suffering of too much connectivity. In such a world, when such an event occurs, the states are practically "paralyzed" for a period of time which we estimate to last between 6 and 12 weeks.

During this period, the reaction of authorities is oriented towards the inside, towards the country's own citizens, towards its own health systems, the interest in internal policy being predominant as compared to external policy. It is the stage in which we notice that we need a lot of things and each is trying to solve in an individual manner what they lack in national economy through imports. Still, "gridlocks" occur in international transportation, as each state took its own measures for restricting the movement of people and transports of goods of all kinds. During this time, at global, regional and national levels, demand is higher that the offer to the products that states' citizens need and a new block-up occurs as well as a rise in prices. This is the period in which we consider that both competition and cooperation tend to decrease towards a minimum, being at a time when "each one is on his/her own".

After this interval, the collaboration and cooperation mechanisms are set into motion (within EU, NATO, strategic partnerships, bilateral agreements etc.), economic-financial and other kinds of decisions are made referring to the citizens of member / partner states and their economies, and we witness a certain return to normality. This is the time when we consider that competition should remain at a minimal level, while there should be a significant increase, towards the maximum possible, in collaboration and cooperation. This does not mean that competition should stay like this in all

---

[25] Barry Buzan, *Popoarele, statele și frica – O agendă pentru studii de securitate în epoca de după războiul rece*, Editura Cartier, Ediția a doua, Chișinău,2014, pp. 153, 155.

domains, as it is bound to become fully visible and very high in the domain of research for discovering the vaccine/ cure to save people from this virus.

Identifying this length of time, as we perceived and described it above, made us come up with the conclusion that, irrespective of the union, alliance, partnership and so on that any state belongs to, if/when such an event happens, there will be a period in which it is going to have to work and function on its own, independently, a period which we called "autonomous functioning|".

That is why our proposition is that the authorities in our country take measures that might lead to the functioning on the national territory of capacities of production capable of ensuring basic utilities, products of strict necessity, equipment of protection, medical devices, tests, medicines etc.

Opportunities occur not only in competition, but also in crisis situations, which should give food for thought to our politicians regarding modifying the profile of our country which is not one of an industrialized country and, at the same time, pay special attention to agriculture which might become one of the „engines" of national economy.

In this sense, Romanian authorities should invest more and more in national economy and stimulate, at the same time, through economic-financial means, the investments in capacities of production of the grand international companies.

At the same time, among the existing production capacities, there should be identified the ones capable of performing reconversion in a relatively short time, in order to produce what we need.

Last but not least, these capacities of production should be part of the national security industry.

The syntagm „utilities and products of strict necessity" can be developed in the Guidelines for National Defense Strategy and the capacities of production meant for the „autonomous functioning" of the state should be established and subsequently comprised in a plan (Plan of capacities of production), an annex to the Plan of strategy implementation.

The „autonomous functioning" of the state also presupposes rethinking the national system of public healthcare, creating a reserve fund which should be intangible to other purposes, beside constituting and maintaining a stockpile of the materials and products mentioned above, within state reserves.

The lines below are going to cover, from our perspective, the beneficial effects of a „White Swan" type of event, as well as one of the features of „Gray Rhino" type of event, namely doing something in order to fix the things that we see happening right in front of us.

In this respect, we consider that there should be a restructuring of global/regional political strategies which might not allow COVID-19 virus affects the relations within unions, alliances, partnerships.

On long term, it is essential to stop the „virus" of apparent selfishness, as during this period each state is forced to manage by itself, as the others cannot help and in case it ever shows up, this virus might be blocked by the "vaccine" of collaboration and cooperation.

This period in which we are expecting more rapid dynamics of relationships within the EU, NATO, partnerships, etc. should not give birth to the „virus" of breaking relations or to the „virus" of dissipation.

On the contrary, it should be defined, formalized through new rules, so that member / partner states might not feel isolated or abandoned, not give births to foolish pride or extreme fears, social fears that are natural in difficult periods and not to be tempted by the „mirage" of helps which, on long term, may prove not to be lacking in traps.

That is why, the EU and NATO member and partner states should support through economic-financial means the development of capacities of production that could ensure each member „autonomous functioning" until setting into motion the mechanisms of collaboration and cooperation.

The plan with capacities of production should be made up to EU/NATO level and the approach we consider most efficient is part of this whole.

A balance should be found between the mechanisms of the free market and the rules of security so that it is clearly stated how far the rules of free market can go and where security rules get into action. Also, it should be stated how far some measures which may be characterized as authoritarian could be taken, so as not to affect medium and long term measures.

„Autonomous functioning" is necessary to each state so as not to become a burden to the other member states of the union / alliance.

Functioning autonomously yet together we are going to be stronger!

At the same time there is a need for changing the authorities' means of communication so as not to allow creating false expectations. This is the job of pragmatism to teach us and to „give us an immunity shot" against unfulfilled human and societal expectations, so as to know exactly what we could do ourselves and what and when we need to wait from the others.

Not having expectations and knowing exactly the possibilities of help from the others are the only means of efficiently countering fake-news and having correct and direct communication with the members of the state's own society. So people will know how, when and until when to help themselves and which the moment is when they might rely on the other partners as well.

If citizens are correctly informed regarding the plan to be applied and if they see that the measures are correct, then they will not get to experience the feeling of social uncertainty whose consequences are going to be extremely hard to erase on the medium and long term.

People are going to be tempted to listen to and credit those who seem to be addressing them directly in order to relieve their fears. This should also result in stopping the „contamination" with the "virus" „Who is to blame?".

Certainly, the coronavirus „…is an opportunity of resetting mentality, of bringing these obvious risks upfront"[26] and it is going to go away „…, but the good part might be that it is going to make people think what kind of world we wish to live in"[27].

If we do not do that, which is quite likely as states' authorities would get to question the efficiency of their own social-economic and political-ideological systems, a possible future fight at global level is going to find us just as unprepared as we have just proven to be.

The crisis is going to pass and a new competition is going to start and whoever is going to be the first to re-start the „engines" of the economy is probably the one to hold world supremacy.

---

[26] Michele Wueker, *[https://revistasinteza.ro>profe....],* accessed on 02.04.2020.
[27] Naom Chomsky, *[https://internal. diem25.org>events],* accesed on 03.04.2020; *[m.youtube. com],* accessed on 03.04.2020.

References

1.	Barry, Buzan	*Popoarele, statele şi frica – O agendă pentru studii de securitate în epoca de după războiul rece*, Editura Cartier, Ediţia a doua, Chişinău.
2.	Isaac, Asimov	*Zeii înşişi*, Editura Teora, Bucureşti 1993.
3.	Nassim, Nicholas, Taleb	*LEBĂDA NEAGRĂ, Impactul foarte puţin probabilului*, Editura Curtea Veche, Bucureşti, 2009.
4.	***	http://descopera. org>teoria-l.
5.	***	http://romania. europalibera.org>d.
6.	***	https://revistasinteza.ro>profe....
7.	***	evz.ro.
8.	***	www.rador.ro>NATO.
9.	***	https://www.presidency.ro>media.
10.	***	https://internal.diem25.org>events.
11.	***	m.youtube.com.

PANDEMIA DE CORONAVIRUS
ȘI SECURITATEA CIBERNETICĂ

CORONAVIRUS PANDEMIC AND CYBERSECURITY

Col. (ret.) Professor Gheorghe BOARU, PhD
Tenured memeber of the Academy of National Security Sciences,
Tenured member of the Academy of Romanian Scientists
E-mail: boarugheorghe@yahoo.com

Rezumat: În această perioadă de criză sanitară gravă de nivel mondial, generată de Coronavirus, organizațiile din sistemul de securitate și apărare națională, dar și o parte dintre cele civile, continuă activitatea în sistem online de la domiciliu sau în sistem telemuncă. Prin acest nou tip de activitate, preponderent online, organizațiile pot crea, din neatenție, o breșă de atac mai largă pentru actorii amenințării cibernetice. În această perioadă „escrocheriile coronavirus" sunt în creștere.

În acest articol voi încerca să atenționez asupra câtorva moduri de a vă proteja Internetul, rețeaua și dispozitivele (devices-urile) proprii. Putem considera acest articol ca fiind un ghid general simplificat menit să surprindă esența a ceea ce aveți nevoie. Sunt prezentate 33 de recomandări practice doar pentru calculatoare nu și pentru telefoane mobile.

De fapt, indiferent dacă este vorba despre COVID-19 sau de o altă situație de criză, nu neapărat sanitară, aceste sugestii consolidează bunele practici și obiceiuri de securitate.

Cele 33 sfaturile sunt chiar concrete și practice și pot fi excelente pentru apărarea împotriva înșelătoriei / exploatării / atacurilor diferite. Urmând sfaturile prezentate în acest ghid de supraviețuire, este posibil să rămâneți neafectați în fața hackerilor și să le zădărniciți acțiunile înainte să aibă șanse de a vă penetra rețeaua informatică.

Cuvinte cheie: securitate software, hacker, amenințări cibernetice, parole, confidențialitate, pirații Internetului.

Abstract: In this period of serious global health crisis, generated by Coronavirus, the organizations pertaining to the national security and defense system, as well as some of the civilian ones, continue their activity in the online system from home or in the telework system.

Through this new type of activity, carried out mainly online, organizations may inadvertently create a wider breach of attack for cyber threat actors. During this period, "coronavirus scams" seem to be on the rise.

In this article I will try to make you aware of some ways to protect your Internet, network and your own devices. We can consider this article as a simplified general guide designed to capture the essence of what you need. Thirty-three practical recommendations are presented only for computers, not for mobile phones.

In fact, whether it is COVID-19 or another crisis situation, not necessarily a health one, these suggestions reinforce good security practices and habits.

The thirty-three tips are concrete and practical and can be excellent for defending your devices and yourselves against various scams / exploitation / attacks. Following the tips in this survival guide, you may remain unaffected by hackers and thwart their actions before they stand a chance of penetrating your computer network.

Keywords: *software security, hackers, cyber threats, passwords, privacy, Internet`s pirates.*

Introduction

The invasion of Coronavirus (COVID-19) surprised and comprised the whole worlds. At the time of writing this article, the situation is quite dreary as most of the important countries have already confirmed a significant number of infected people, serious cases and a lot of deaths. Romania was unfortunately not excluded from this serious health crisis.

As the state of emergency and later on the state of alert were instituted by decree, acknowledging the existence of the pandemic in Romania, unprecedented social restrictions were applied, leading to the necessity of adjustment and finding new ways of carrying out social activities and actually people's lives.

Thus, some of the state and private institutions continued their activity online embracing online working or working from home.

Continuing to fulfil their job-related duties online, employees (and also the managers) may forget to take special technical and organizational measures thus increasing the vulnerability of operations including the information that is transmitted through the cyber space.

Becoming aware of the importance and the dependence on this cyber space, much increased because of current circumstances, people started to think it is essential to provide enhanced security to it and to all IT and communication systems. Thus, we have in mind the fact that „*...in analyzing a military information activity, information can be considered*

„raw material”, „purpose”, „target”, „weapon” and that is why protecting it is even more important and complex”[1].

Through this new type of activity – with everybody working from home – organizations may carelessly create a wider attack area for the Cyber Threat Actors - CTAs.

IT departments in institutions pertaining to the field of security and national defense needs to remain vigilant as, at the most basic level, malwares and hacking instruments have also become more easily available allowing those who are not necessarily IT specialists to understand and use them correctly.

„The existence of this virtual environment or **cyber space, recognized as a conflict environment, is based on the successful exploitation of the dependence on data and information***, manifest at the level of military structures, all the more so as it acts in a hybrid conflict environment. Besides the automatization of actions and the digitalization of military forces, civil society has contributed to increasing the dimensions and defining cyber space as the fifth conflict environment, next to the land, air, maritime, and cosmic ones”[2].*

In case of creating these breaches of security, criminal hackers and underground networks can take advantage of this situation in order to attack vulnerable targets and their infrastructure systems.

These are times when *„coronavirus scams”* are increasing in number. They include actions performed by the same cyber security professionals who are known for their past similar actions. Or maybe they are new ones, but they are actually alike. The main difference is that they are operating under *"corona"* premises.

The IoT domain (**I**nternet **o**f **T**hings)[3], which is a constant presence in the preoccupations of IT specialists has two major types of application,

---

[1] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare „Carol I’, București, 2018, p. 6.
[2] Gheorghe BOARU, Benedictos IORGA, *IMPLICAȚIILE PARTICIPĂRII FORȚELOR MILITARE ROMÂNEȘTI LA OPERAȚIILE DE TIP COALIȚIE, ASUPRA EVOLUȚIEI ȘI DEZVOLTĂRII SISTEMULUI MILITAR NAȚIONAL DE COMUNICAȚII ȘI INFORMATIC*, Editura SITECH, Craiova, 2020, p. 236.
[3] IoT (**I**nternet **o**f **T**hings) is a quite wide definition, covering essentially any device that is capable to communicate with other devices on the Internet. Actually, every day there are

that in the consumption space and those in industry (civilian and/or military organizations). Tens of scientific papers have been published only this year regarding IoT, the authors[4] being from all continents. All papers are also focusing on the security of these systems.

The guide with recommendations include a wide range of attack possibilities such as phishing, ransomware and fake advertisements. Governments, enterprises, and natural persons need to become aware of them and look for ways to stay safe.

Nowadays turmoil may turn you into a target. Maybe there are a lot if important details in the information hackers are looking for. Protect them and look for ways of consolidating your own security. At institutional level „*the global and multidimensional character implied by ensuring information security, acknowledging the necessity that security governance is developed in order to counter the cyber threat, leads to the necessity of engaging several levels, actors, institutions and people involved in the cyber ecosystem*"[5].

In this article I will try to raise awareness regarding some ways of protecting the Internet, the network and your own devices. The article covers topics such as email, passwords and software security. It may seem

---

more and more gadgets and devices that are connected to the Internet. This means bigger opportunities for cyber attacks. The more developed IoT is, the more security issues may occur regarding information and information systems.

[4] Huimin Lu, *Cognitive Internet of Things: Frameworks, Tools and Applications,* Series: Studies in Computational Intelligence 810, Publisher: Springer International Publishing, Year: 2020; Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdizadeh, Farhad Norouzi, *Towards the Internet of Things: Architectures, Security, and Applications*, Series: EAI/Springer Innovations in Communication and Computing, Publisher: Springer International Publishing, Year: 2020; Sheng-Lung Peng, Souvik Pal, Lianfen Huang, *Principles Of Internet Of Things (IoT) Ecosystem: Insight Paradigm,* Series: Intelligent Systems Reference Library Vol. 174, Publisher: Springer, Year: 2020; Srikanta Patnaik, *New Paradigm Of Industry 4.0: Internet Of Things, Big Data & Cyber Physical Systems,* Series: Studies In Big Data Vol. 64, Publisher: Springer, Year: 2020; Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment,* Publisher: Apress, Year: 2020.

[5] Col. (r.) prof.univ.dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană*, Revista Academiei de Științe ale Securității Naționale, nr. 2/2017, p. 68.

general, but actually all this advice is excellent as a means of protection against different attacks/ exploitation / scams. The issue is by no means new. *„Thus, in 1985, a 25-year-old Chinese military, Shen Weiguang, wrote an essay called „Information Warfare". In this article he approached notions such as „information border", „information factory", „information-based army", „information police", „home combat" and described information as the most significant feature of society"*[6].

Actually, irrespective if we are referring to COVID-19 crisis or another emergency situation, these suggestions consolidate the good practices and habits of security.

I cannot produce evidence with respect to the fact that SARS-CoV-2 virus was produced in a laboratory by X or Y world actor and used as a „biological weapon" but I can surely say that IT viruses are the results of the work of extremely skilled specialists who, for certain individual or group benefits, cause direct or collateral damage to regular users who do not know or apply the basic "hygiene" rules.

 At national level, the regulations regarding the protection of information define the domain with sufficient clarity. Romanian cyber security strategy defines cyber security as *„the state of normality resulting from applying a number of proactive measures meant to ensure the privacy, integrity, availability, authenticity, and non-repudiation of information in electronic format, public or private resources in the cyber space"*[7].

You can choose to implement any of these pieces of advice or at least understand the reasoning behind them. These suggestions focus on practices and things that can be done right away.

We may consider this article as general simplified guidelines meant to expose the very essence of what you need in this field. If you consider it necessary, you can read more and go deeper in all these issues. Actually, responsibility belongs to each of us. We should remember the words of

---

[6] Col. (r.) prof. univ. dr. Gheorghe BOARU, *RĂZBOIUL INFORMAȚIONAL – UN OBIECTIV AL SECURITĂȚII NAȚIONALE*, Revista Academiei de științe ale Securității Naționale nr.2/2019, p. 29.
[7] Decision no. 271/2013 regarding the approval of *Romanian Strategy of Cyber Security and National Action Plan for Implementing the National System of Cyber Security*, published in Romania's Official Gazette, Part I no. 296 of 23.05.2013, p. 7.

former American President Abraham Lincoln: „*One cannot avoid the responsibility of tomorrow by eluding it today*".

Thus, the following series of rules regarding the personal obligations of Internet users turned into a Guide with 33 recommendations, just as another specialist suggests[8], but also advice adapted to the Romanian circumstances generated by Coronavirus.

Cyber security – Recommendations for users

1. Adopt stronger passwords

User names and weak passwords are often the best combination that hackers take advantage of in order to breach vulnerable accounts.

Many users use passwords such as „1234" or „111111". Such weak passwords may be guessed or broken very easily.

The solution is to devise your own system for creating new passwords. Mix special characters, figures and letters in order to make the account access more complex. Moreover, try not to use the same passwords several times and for different accounts. Thus, if an account is broken, the others are not going to be affected.

2. Choose cautious privacy policies

As websites constantly change the way in which users get connected and the manner in which their data are collected and stored, the General Data Protection Regulation and other legal frameworks established the manner in which companies had to update the way they collect data. Websites are going to examine data in order to identify tendencies and predict the users' behavior.

What can be done? Every time you get connected to a website, visit their privacy page. Read their policies regarding data collection and what they do with dese data. Look for and carefully understand technical jargon.

If the websites you visit or buy from do not have a privacy policy, consider it as a sign that you should be careful.

3. Anticipate cyber attacks

---

[8] LEVI WEST, *The Coronavirus Cybersecurity-Survival Guide-Top Tips to Protect You from A Cyber Attack,* 2020.

Hackers permanently look for means of creating breaches in IT systems. Cyber-attacks occur every day. A large number happens due to computerized automatization used in many domains.

What can be done? If cyber-attacks can take place at any time, then users need to update and to protect their systems as fast as possible. Run the antivirus soft automatically. Scan all new files that you download to make sure that they do not contain malware. Never install anything that you are not familiarized with and especially that seems weird (too cheap, free, too helpful, even "life-saving").

Ban access to your valuable information through passwords. All operation systems will allow you to also hide folders.

4. Avoid suspicious offers

The people skilled in creating tempting offers create on the Internet a feeling of urgency and lack of certain products in order to make users buy fake products, download their free software (which is infected) or introduce the information regarding their credit cards on fake sites.

What can you do? First of all, do not panic. These sites and these "sellers" are configured with "new" products that do not exist. They may create fake offers which have no connection to reality. They can promise, for instance, a treatment or immunity formula even for COVID-19 (naturist cures, medicines, vaccines, etc.). I found someone on the Internet who was trying to sell anti-Covid-19 sprays. Interesting, right? Beware of suspicious advertisements and promises that sound too tempting to be true.

Clickbait is one of the cheapest ways through which hackers and sellers of different products find out information and even gain money in an illegal way. They will be presented as "once in a lifetime offers". For instance, there were offers of Covid tests for 100-150 RON, ordered on the Internet. These offers sounded very tempting as they said they could be used at home and results can be obtained almost on the spot. Emotions are speculated at different moments, in this case, for instance, when these official testings were not available to the large masses of population (for both technical and political reasons) and fraud money can be thus obtained, without having the possibility to fulfill the promises specified in the respective generous offer.

In this pandemic period and given the Military Emergency Ordinances, when school takes place online, the Internet is filled with

interactive online lessons and games (texts, graphs, films, etc.) offering malicious Internet users the possibility of penetrating systems and taking advantage of the situation for hacking purposes. „The Pirates of the Internet" exploit the moment and go about their business undisturbed if you have not taken the necessary measures to secure the devices you use. These people even have a flag (in several variants) having as a common element the pirate symbol (see Figure 1).

Figure 1. Pirates' flag on the background of the blue sky

Actually, through its own definition, the concept of **hacker** refers to *"...an expert in* <u>*informatic*</u>*s, who deals with the profound study of IT programs (*<u>*operating systems*</u>*,* <u>*applications*</u>*), often using techniques of* <u>*reversed engineering*</u> *(dismantling), with the aim of acquiring knowledge that is not accessible to the wide public. Those who use this knowledge for illegal purposes, in order to compromise the* <u>*security of IT systems or applications*</u> *are actually* **crackers***, but in the public's perception (usually created by* <u>*mass-media*</u>*) the notions of hacker and cracker are often mistaken one for another*[9].

From the latest works in the field[10], we have come up with the conclusion that a hacker can be defined as „*The person who uses computer technology in order to get unauthorized access to information or to manipulate informatics systems of to obtain illicit material gains"*.

---

[9] *[https://ro.wikipedia.org/wiki/Hacker].*
[10] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics,* Publisher: Harvard University Press, Year: 2020; Vinny Troia, *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques,* Publisher: Wiley, Year: 2020; Aditya Gupta, *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things,* Publisher: Apress, Year: 2019;Jim Kou, *Hacking: The Practical Guide to Become a Hacker | Field Manual for Ethical Hacker Including Ethical Hacking with Kali Linux,* Publisher: Independently published, Year: 2019.

5. Make spare copies of your data

A Murphy Law says that „*if something may go wrong, it will*"[11]. As a user, you should have a reliable copy of your data well stored in case something does not function right. The possible reasons may vary from the physical destruction of your computer up to a broken hardware ion case of a cyber-attack. You may never know when your smartphone or the hard disk from your computer turn out completely dead. A second "life" will rapidly change the situation.

What can you do? Think about the data you have and what exactly they count for. Rank them from the most important to the least important ones in order to establish the order in which you will create a back-up for them. After doing so, store the data on a reliable cloud network system and on another device / system that you have. Make sure they are the most appropriate external memory devices for your needs (CDs, DVDs, BDs, memory sticks, external hard disks, etc.).

The recommendation is to make regular and continuous backup.

6. Pay attention to phishing

Phishing is another popular tactic used by hackers to have access to the victim's system. Phishing implies *masquerading* (disguising, hiding one's real identity) in order to gain your trust and steal your information. They may pretend to be your favorite company, your boss, or even your friends. The most encountered method is via email, but it can be done through any means of electronic communication.

What can you do? If you notice something strange, be careful and check it out: is the quality of the email the same? Is there anything wrong with it? A lot of phishing emails will ask you for personal information and will persuade you to answer back. Real and serious companies do not ask for this kind of information in an email.

Never answer this type of communication. Phishing is simple, but it is one of the most dangerous types of attacks.

Phishing takes different shapes. Because of the low costs of transmission, hackers usually send phishing schemes to catch their victims. I am going to briefly describe two of the most common types of phishing.

---

[11] *[https://www.academia.edu/21702040/Legile_Lui_Murphy]*, cap. 3.

Spear phishing. This is a sophisticated type of phishing targeting a certain person and a certain email account. In this particular situation, the hacker knows pretty much all there is to know about the victim. They can even study the victim's behavior and can determine the best moment of the day to catch him/her off guard, in a moment that is favorable for the attack. Thus, when a spear phishing attack is launched, it will seem very real and relevant.

Whale hunting is a type of phishing targeting the management and the levels of leadership of an organization. Hackers do their research on social media platforms such as *LinkedIn*[12] and identify the partners they work with.

Concomitantly, when they send emails, hackers can enclose links or relevant attachments for the daily operations of an organization. When it is opened, this will compromise the system through malware (such as a virus or a *Keylogger*[13]).

So, refrain from disclosing private information as much as possible and in any circumstances possible.

7. Check emails twice

Why is it important? Cyber criminals know that their potential targets may give in to panic or impulse. Due to this possibility, they know that when sending a malicious email, it is quite likely that it is going to be opened.

What can you do? Whenever you receive an e-mail in your mailbox, check the sender and the mail address used. Make sure that mail address is one that you have already used for sending and receiving emails to / from. Cyber criminals can create a false domain and add characters in order to seem legit. For instance, user@un.org is an official domain of

---

[12] *LinkedIn* is a social network oriented towards the professional environment with the help of which any user can find a job or any employer can find the professional he/she needs.

[13] A *Keylogger*, also called sometimes a system monitor, is a type of surveillance technology used for monitoring and recording each key pressed on the keyboard of a computer. Keylogger software is also available for smartphones, such as Apple iPhone and Android.

United Nations. So, it is highly unlikely to receive emails from addresses such as user@un-safety.net or user@un-usa.com.

8. Check spelling and grammar

Why is it important? It may seem obvious, but a lot of hackers make spelling or grammar mistakes when they communicate with the potential targets. There are a lot of international hackers who learned English as their second or third language (if we refer to messages written in English). Many of their fake emails may sound funny or include phrases that a native speaker would very rarely use.

What can you do? If you receive something suspicious from friends, workmates, former comrades etc., take wording into consideration. Is it awkward? Is it far-fetched? Was the message sent at an unusual time for conversations? Would you say that person sending you the email usually has this type of communication with you? Romanian language is complex and, in this case, this is good as false friends will surely reveal themselves as being so by turns of the phrase or expressions that are unnatural for our language. If the text of the messages is in another language (such as English) then resort to a translator or to a person that knows that language well enough to realize such elements of subtle detail.

No one is perfect. This is true also about hackers.

9. Avoid fake Coronavirus plans (maps)

Using maps and graphs is one of the best ways of making a story seem credible. Every time the media tries to refer to the current state of the virus, they will present a geographic map or data – such as figures or images – in order to offer a relevant picture of what is going on.

Due to the population's trust in this kind of information means, hackers copied the format and incorporated malicious links in order to steal information from you.

What can you do? Mark your official and known sources, so as to be able to resort to them only when there is a need to do so. Your source of information has to be reputed news sites and official sites. Never underestimate the creativity of a hacker!

10. Do not open suspicious emails

We constantly receive unsolicited and unexpected emails. They are sent as news, advertisements or important announcements. They may seem tempting, but it is obvious that you must not click on the suspicious emails;

yet it may happen to anyone to forget this rule. Opening them may offer hackers sufficient information about you, even if the click was made out of curiosity. For instance, they may find out where you are and even get your exact location.

What can you do? Report any mail that you receive unexpectedly in your mailbox to authorities and / or the email provider.

Configure another email account to use as a buffer between the newly created account and your main account.

After configuration, activate an email pre-visualizing setting which isolates the content of your main account.

11. Do not click on suspicious links

Even if you are opening an email from a trustworthy contact or source, hackers can still compromise your system. Actually, there are many instances in which they first compromise the systems of your family and friends as this enhances the chances that you might read their emails. However, it might be difficult for them to compromise these accounts. Instead, what they may do is redirect web hyperlinks (the blue links) which you see in emails towards another location they control. A false account on the website of your bank or on a social network that you use, for instance.

What can you do? You should avoid to click on the direct links that were incorporated in the emails. Copy the link, otherwise known as Uniform Resource Locator (URL) and put it through a URL scanner. Sites such as *virustotal.com* and *sucuri.net* are popular for this reason.

Malicious links are some of the most common vectors used for fooling the victims.

Why is it important not to click on suspicious links: these links are a common denominator for hackers to obtain unauthorized access. Hackers are often going to use abridged links capable to redirect you towards harmful websites.

The abridged links use a number of characters with a very short length. Yet, hackers have realized that it is difficult for someone to see and check a connection as these links may be quite confusing.

What can be done? When you receive suspicious links, examine each of them carefully. Use URL scanners to check if they are malicious. Despite its shape, it is actually a link. If you have to, open the email before

copying and inserting the link in the URL scanner in order to establish whether it is safe or not.

12. Download security programs

This is a security instrument which is always necessary for protecting your information systems. This instrument also needs to include a number of protection software such as antivirus, anti-spyware and a powerful firewall. Each of these is an integral part of your defense.

What can you do? Find out what you can afford and which the price is. You can find a lot of good antivirus and anti-spyware programs, but most of the more solid and updated ones require subscription. Only you can decide upon the most convenient product both cost-wise and from the point of view of the protection offered.

13. E-mail attachments can be dangerous

Malicious attachments can be an efficient means of infecting the IT systems of a certain user. The attached files, although simple ones, can also host executive malware that may rapidly compromise your information. It does not matter if they take the shape of a document, a calculus table or even an image. All these may prove to be harmful.

What can you do? If you have a setting which automatically downloads attachments, stop it right away. Make sure that any attachment you get is an attachment that you expect. For instance, if a colleague from work said that he/she was going to send you a certain file, then you will know that it is coming. Yet, scan each file as soon as it gets to your mail box in order to put your mind at ease. Do not necessarily trust your instincts, check any file even if you did not use to do so before the pandemic.

14. Avoid Ransomware

Ransomware is one of the main cyber threats that are used against innocent victims. Ransomware is a type of malware that blocks all the data of the victim and encrypts them so as the respective person might not have access to them. They infect computers in many ways, but the already mentioned opening of unscanned attachments or visiting already infected sites are two of the most important ways.

Once the system infected, the hackers will ask for money as ransom (Euro, USD or usual crypto coins) or else threatening to reveal the data publicly or erase them completely.

What can you do? Remember that talk about data backup? Fresh backup represents one of the best defenses for your data. If they erase your data, you can turn to the copy you have made and continue to operate normally.

Ransomware is an old but extremely efficient threat.

Treat it seriously!

15. Make sure you have installed the most recent firmware

The firmware is a software incorporated on your hardware to help it work. There are a lot of Internet users who fail to update the firmware activated on their router. This exposes their network to security flaws that may be used by the hackers taking advantage of distance users.

What can you do? Connect to the software for managing the Wi-Fi and conduct an update on your router. Install the most recent software if you know you have got an outdated one. Check if your router has an automatic update or if you can set it up for automatic updates. In addition, resort to the Internet service provider for supplementary advice regarding the router and the Wi-Fi network. Try to purchase other devices, more modern, as the case may be.

16. Expect the social media to be overwhelming during this pandemic period

We are living in an information era. We are completely relying on the Internet to see what is going on. The first thing people resort to is social media. Social media is the largest vector of infecting media users. There are a lot of false accounts (administered by computer bots) and there are a lot of entertaining news that are going to take a serious amount of your time which would normally be used for accomplishing the tasks on which you are working from home.

What can you do? Minimize retweets and share only the relevant posts. Only flow a limited number of sources for news. *Signal and report any kind of fake accounts!*

17. Fake videos through DeepFakes

Streaming media is a multimedia material which is permanently received and presented to a final user while being delivered by a provider.

Streaming is a double-edged sword. On the one hand, data knowledge and automated learning have allowed to rapidly find the videos that we consider relevant and informative. Yet, the hackers and the

manipulators of social media have also created fake videos called "deepfakes".

The notion of deepfake means that a video clip is thus altered so as to bear all the features of an authentic one. For instance, the face of a person on a clip is changed with the face of another person. Due to coding details, these clips seem very real and convincing. This allows hackers to control national conversations and online debates. Some are actually state of the art deceit.

What can you do? Think twice about the clips that seem suspect or surreal. Check the image to see whether there is some light that falls in a wrong way or if the clip is not fully synchronized. Many of the existing deepfakes are very close to reality, but in fact inexact. Usually, there is something wrong with them as the algorithms creating these clips are not perfect either.

When in doubt, „dig" deeper!

18. Pay attention to fake charity actions for Coronavirus

There are lots and lots of new websites created by organizations that pretend to deal with charity work, including in the names a combination of words among which "victims" or "alleviation of suffering".

These words are meant to stir natural emotions among users. Many of these domains are actually harmful and are going to install some software on your computer so as to spy on your accounts and your web activity.

What can you do? If you intend to donate for emergency aid, check on the respective charitable organizations before doing so. Make extensive research on the potential of the charity organization you may donate to. Examine their records in order to see their reviews and look for clear documentation on their history.

19. Beware of Cyberbullies

The Wild West atmosphere on the Internet also offers space to evil doers who might find a new way to harass the others, anonymously posting malicious information. Sometimes, these comments may turn in physical actions with consequences in real life.

What can you do? In order to deal with a cyberbully, there are a series of things you can do. First of all, limit the amount of personal information you upload in the virtual world, so as to be really hard for anyone to harm you or expose you online.

They will look for you on Google or on the sites of different blank pages in order to see who you are and expose you online for everyone to see. No matter what you do, do not escalate the situation answering with hostility. Finally, look for useful data and record the entire activity you carry out. This will help you with reporting and taking legal action in case you choose to do so.

20. Identity theft

Millions of people have been affected by the theft of identity. The theft of **P**ersonally **I**dentifiable **I**nformation - PII, such as contact data, travel documents data or the date of birth offers a significant amount of ways through which hackers can make good money. When you introduce such details in any IT device, you risk that a hacker steals this information and use it for fraudulent actions.

What can you do? Avoid to provide PII unless it is absolutely necessary to do so.

It is difficult to make sure how safe your information is in a bank, in a hypermarket, and so on. You only have one identity, so you need to find ways and means to protect it.

Monitor your credit and be prepared to freeze it at any moment.

21. Implement the authentication with two factors

Why is this important? The authentication with two factors is a mechanism in which two separate kinds of information should be presented in order to be allowed access to an account. For instance, in order to access your bank account, it might be necessary to provide both the password and a special, unique code delivered to you by your mobile phone (Mobile Token). This supplementary security level makes it difficult to compromise your account even if your password is listed somewhere on the Dark Web.

What can you do? Go over all the applications and services that you have used, especially those related to financial information. Check if each of these have two factor authentication. Try to activate this option on as many applications as possible. It may be perceived as an inconvenient and it may take some time from your workday, but it is worth doing it so as not to have problems when you are trying to prevent the disruptive endeavor of a hacker.

Beyond the authentication with two factors, there are also possible authentication facilities with three or four authentication factors.

22. Find out about Scareware

Just as the name *scareware* suggests (being derived from to scare, frighten, deceive), this is a type of malware that aims at taking advantage of the user's anxiety.

Scareware does this by launching a terrifying message that is going to threaten a user to do something contrary to his/her interest. Thus, money will be required in exchange.

What can you do? Using a good antivirus program is a good idea for scanning the type of threat.

Scareware is a known threat and the renowned antivirus companies have built protection against this kind of threat. Make sure that you access only the trustworthy sites and do not be afraid. A lot of scareware has been used several times. It is possible that this multiple use is what makes it vulnerable at some point.

23. Log off frequently!

Personally, maybe you like it sometimes to stay connected for a long period. The best idea is, after closing your work session, to erase the credentials. This will allow you to narrow down the window of opportunity that a hacker has. Actually, many hackers use hijacking sessions (credentials stocked for too long) as a modality of stealing someone's identity.

What can you do? Disconnect any services you might need while working, especially those related to financial information. The automatic connection functions that are saved by the accounts should be permanently deactivated. Irrespective if you use a laptop or a smart device, this type of functions offers hackers an advantage if you end up losing control of your data.

24. Maintain your communication with the employer

This piece of advice is rather addressed to the people working from home. So, if you are working, you had better not isolate yourselves, but, on the contrary, keep the pace with the continuous evolutions and changes in security policies. These updates are actually visible at every step on the IT market.

What can you do? Make a list of job related contacts and obtain people's email addresses, phone numbers and other contact data. Keep a list with all the questions you might have. For instance, look for clarifications regarding the manner of recording connection data and what is actually

considered to qualify as working from home. At the same time, find out who is the contact designated for specific problems, such as assistance problems. Find information about IT issues that are going to offer you a good working pace, without security incidents.

Working from home, which might take longer than it was initially anticipated, may extend the vulnerability to an attack that a hacker may exploit.

25. Not all VPNs are safe

The virtual private networks or VPNs are a common modality of encrypting certain traffic on the Internet. Due to the necessity of working from home or protecting information, many news articles suggest the use of a VPN (V*irtual Private Network*).

The problem is that not all VPNs are safe, many of them being run by hackers.

What can you do? If you decide to use a VPN, make sure that it has been reviewed by others. Some of the best VPNs have hundreds of reviews, and even awards. It is necessary to pay for their services if you want a high quality service.

26. Public Wi-Fi networks are vulnerable

Any time you get connected to a Wi-Fi[14] in a public network, you are actually exposing your data to somebody else. This may happen when you are working from different places. Unlike your private network, that you use at home, you will never know who is getting access to a public network at a certain time. Hackers may intervene in the connection and steal your information.

What can you do? Generally speaking, avoiding public networks is the best way to act. As you do not have enough control over them, you cannot tell what may happen. However, if you absolutely have to get connected to one of them, it is best not to access sites that are sensitive to your online identity (online banking, social media accounts etc.). Deactivate file sharing and make sure you log out of all accounts when you have finished.

27. Scan the new files

---

[14] *Wi-Fi* is a radio technology often used for implementing the *Wireless Local Area Network, WLAN.*

We have already touched upon this topic regarding email attachments, but the same goes for all the new files you receive in your system. They may be from the Internet, just as well as they may be from a USB or CD unit. All new files should go through the same process.

What can you do? Right after you obtain a new file, isolate it and scan it. If you download and use security instruments, that you can *click right* on the file and *scan*. Make sure your antivirus software is updated to be sure that it is efficient in detecting the known malware signatures.

Better safe than sorry!

28. Stop disinformation

We are all constantly bombarded with information and disinformation.

What can you do? Be ready to remark, note down, and tell others of this inexact information circulating on the Internet. Report dangerous information to the adequate channels (the authorities) in order to see if measures can be taken. There are a lot of private companies that will answer quickly and easily take over your information. Think about online volunteering service or resort to certain organizations in order to offer your help.

29. Prepare yourselves and get some training in the domain of information security

Although it may seem a simple matter of raising awareness in security matters, training will actually prove really beneficial to you. Preparation and training will create the grounds for combatting these threats. There is always a new trend that occurs in the fight for cyber-security and you should take all of them seriously when they occur.

What can you do? Look for online companies and renowned providers that offer awareness-raising training. There are a lot of such "courses" made online and free of charge, for "students" to be taking from home. Think about the time you might be able to allocate them and if they fit your level of knowledge. Pick one or two initial training courses comparing them in order to obtain the most appropriate practices you need.

30. Pick a password manager

A password manager is another tool that you can download to help you follow all the passwords you use.

However, it is not a complete or final solution. Users will have hundreds of passwords throughout their lives. Password managers organize passwords and make accounts more efficient.

What can you do? Examine the free tools and the options that need to be paid for offered by password managers. The free range is not going to offer the number of solid functions that you would get for the paid for version, but you will be able to obtain them quickly and your bank account will be safer.

The companies for password management often have a free available option. Use what you consider appropriate for your needs.

Password managers are vulnerable too, at some extent.

Never put all your eggs in one basket!

31. Warn others

Every once in a while, it is possible that you might notice something suspicious online. While you are aware of it and so you are not going to fall prey to a harmful activity, expect others to be in danger. You are capable of making the difference.

What can you do? Report anything you think is suspect on the appropriate channel. If it has come to you via e-mail, report it to the e-mail provider. If it is through social media, report it to the company that manages it. Better safe than sorry.

Billions of pieces of information have been stolen and compromised and this number is going to grow as the dependence on the Internet is growing too.

32. Follow the prices

There are a lot of goods and services that were at some point easily available and that have become rare nowadays. This led to e market with over-inflated prices. Some sellers who might be characterized as actual thieves are selling – in full pandemic period – toilet paper, protection masks and gloves or disinfectants at outrageous prices.

Due to this dynamics, the hackers who have resembling sites are going to lure the buyers with merchandise that actually does not exist. These are called *nondelivery* (non-shareable) scams.

What can you do? Research all the web sites before accessing all these offers for information. The safe option would be to resort to providers you have already tried before and that you trust. I am sure that you know that some of these sites cannot deliver the goods you are looking for and/or purchasing for the simple reason that they do not have them.

33. When you can, do not hesitate, encourage good habits!

You have already acquired a lot of information from this article and from your experience. If you have knowledge that you can share with others, do not hesitate, help them take advantage of this, too.

What can you do? When you discuss with others about how to be much safer regarding the protection of information, see if there is something you might help them with or, in turn, be helped by them. Do not hesitate to offer them some of the advice comprised in this article.

Knowledge is power!

Conclusions

Following the advice presented in this guide for survival, you may remain unaffected by hackers and disrupt their actions before even having a chance to penetrate your network.

At national level, in full agreement with European actions, in February 2015, the *National Strategy regarding the Digital Agenda for Romania 2020*[15] was approved, which defines four domains of action among which only the first domain comprises: e-Government, Interoperability, *Cyber Security*, Cloud Computing and Social Media.

Irrespective whether we are speaking of general cyber threats or cyber threats brought by „*Corona",* you can easily find the peace of mind needed for survival and performing in these changing times.

For the domain of security and national defense, according to the estimates of contemporary military specialists, expressed in a work in the field, „*besides the lack of borders, at the level of the new environment in which human society is functioning, other characteristics are overlapping, such as the anonymity of the actions conducted, the legal gaps, and last but not least, the possibility of carrying out actions in the permanent virtual environment, from any place, not being conditioned by certain physical presence or availability of major financial and technical resources"[16].*

These recommendations can help you directly. Thus, you are going to be prepared in advance as you are going to have an updated software that

[15] *Strategia Națională privind Agenda Digitală pentru România 2020* (National Strategy regarding the Digital Agenda for Romania 2020) was approved by Government Decision no. 245/7 April 2015.
[16] Gheorghe BOARU, Benedictos IORGA, *op.cit.,* p. 239.

is going to scan threats as the „enemies" are going to attempt to break into your system. The computer you use will detect the anti-spyware and anti-virus protection to quarantine and isolate the folders that are targeted.

You will hesitate to offer personal and financial information to other people. The identity that you have is an asset and the theft of identity is something you should always be warned to be wary about.

You will not be afraid to deal with an e-mail, as you know the different ways in which hackers can affect you. Be it through spear phishing, embedded links or harmful files, you are aware that you are facing a threat. Thus, you will be able to help the other colleagues when and if they need it.

Regardless whether it is about counseling or reporting fake news, you have the necessary information to identify manipulation.

And, maybe most important of all, you will become more and more interested in finding out supplementary information on cybersecurity. Your opinion on technology and on your own abilities will become higher as they thus grew in a rapid and concise manner. Thus, you are going to have the satisfaction that you have made the Internet a safer place and that, in a critical situation, you can make the difference – in favor of the security of information you are dealing with.

I consider that our experts (both civilian and military) need to find the most appropriate ways of exploitation of the own developed capabilities, specific to warfare, to be used in the cyber-sphere, as well as the necessary technology and doctrines for defending ourselves against cyber-attacks.

According to the opinion of the Chair of the Foreign Investment Review Board, David Irvine BA (Hons)[17], …„*The answer to cyber-threats is going to be complicated not in the least because prophylaxis inevitably remains the resourcefulness of those who use the Internet for harmful purposes.*

This is going to imply sophisticated technical solutions for protecting our connected cyber devices against infiltrations and harmful activity; this will in turn determine cultural or behavioral changes in the

---

[17] David Irvine BA (Hons)- Președinte al Consiliului de revizuire a investițiilor străine, AO (din 2017), Director general la Organizația australiană de informații de securitate (2009–2014), Director general la Serviciul Secret de Informații Australian (2003–2009).

manner in which we react to cyber threats; this will bring about legislation that is going to compel the industry and the IT service providers to protect both the confidentiality and the viability of the critical infrastructure that is now depending on the cyber space"[18].

We need to dedicate more and more intellectual effort to analyzing the impact of these technologies, the vulnerabilities they create and the optimal way of mitigating vulnerabilities. This intellectual effort should also be directed towards the ethical and moral dimensions, as well as the obligations of the appropriate state entities to protect the privacy and safety of its citizens against catastrophes that might be caused by cyber attackers.

References

1.	* * *	Hotărârea nr. 271/2013 pentru aprobarea *Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013.
2.	* * *	*Strategia Naţională privind Agenda Digitală pentru România 2020,* aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.
3.	Col. (ret.) prof.univ. dr. Gheorghe Boaru	*Securitatea cibernetică în Uniunea Europeană*, Revista Academiei de Ştiinţe ale Securităţii Naţionale, nr. 2/2017.
4.	Col. (r.) prof. univ. dr. Gheorghe BOARU	*RĂZBOIUL INFORMAŢIONAL – UN OBIECTIV AL SECURITĂŢII NAŢIONALE*, Revista Academiei de ştiinţe ale Securităţii Naţionale nr.2/2019.
5.	Gheorghe Boaru, Iulian Marius Iorga	*Securitatea sistemelor informaţionale militare*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2018.

---

[18] Henry Prunckun, *Cyber Weaponry - Issues and Implications of Digital Arms*, Series: Advanced Sciences and Technologies for Security Applications, Publisher: Springer International Publishing, Year: 2018, p. VIII.

6.	Gheorghe BOARU, Benedictos IORGA	*IMPLICAȚIILE PARTICIPĂRII FORȚELOR MILITARE ROMÂNEȘTI LA OPERAȚIILE DE TIP COALIȚIE, ASUPRA EVOLUȚIEI ȘI DEZVOLTĂRII SISTEMULUI MILITAR NAȚIONAL DE COMUNICAȚII ȘI INFORMATIC*, Editura SITECH, Craiova, 2020.
7.	Ben Buchanan	*The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics,* Publisher: Harvard University Press, Year: 2020.
8.	Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler	*Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment,* Publisher: Apress, Year: 2020.
9.	Aditya Gupta	*The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things,* Publisher: Apress, Year: 2019.
10.	Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdizadeh Farhad Norouzi	*Towards the Internet of Things: Architectures, Security, and Applications***,** Series: EAI/Springer Innovations in Communication and Computing, Publisher: Springer International Publishing, Year: 2020.
11.	Alexander Klimburg	*National Cyber Security-Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), Publication, Tallinn, 2012.
12.	Jim Kou	*Hacking: The Practical Guide to Become a Hacker / Field Manual for Ethical Hacker Including Ethical Hacking with Kali Linux,* Publisher: Independently published, Year: 2019.
13.	Huimin Lu	*Cognitive Internet of Things: Frameworks, Tools and Applications,* Series: Studies in Computational Intelligence 810, Publisher: Springer International Publishing, Year: 2020.
14.	Srikanta Patnaik	*New Paradigm Of Industry 4.0: Internet Of Things, Big Data & Cyber Physical Systems,* Series: Studies In Big Data Vol. 64, Publisher: Springer, Year: 2020.
15.	Sheng-Lung Peng, Souvik	*Principles Of Internet Of Things (IoT) Ecosystem: Insight Paradigm,* Series: Intelligent Systems

	Pal, Lianfen Huang	Reference Library Vol. 174, Publisher: Springer, Year: 2020.
16.	Henry Prunckun	*Cyber Weaponry - Issues and Implications of Digital Arms*, Series: Advanced Sciences and Technologies for Security Applications, Publisher: Springer International Publishing, Year: 2018.
17.	Vinny Troia	*Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques* Publisher: Wiley, Year: 2020.
18.	LEVI WEST	*The Coronavirus Cybersecurity-Survival Guide-Top Tips to Protect You from A Cyber Attack,* 2020.
19.	* * *	https://www.academia.edu/21702040/Legile_Lui_Murphy.
20.	* * *	https://ro.wikipedia.org/wiki/Hacker.

LIDER ȘI LEADERSHIP MILITAR

MILITARY LEADER AND LEADERSHIP

Col. (ret.) Professor Ion MITULEȚU, PhD
Tenured member of the Academy of National Security Sciences,
E-mail: mituletuion@yahoo.com.

Rezumat: Mediul de securitate actual, multidimensional, înalt tehnologizat, interconectat și interdependent, marcat de amenințări difuze care generează instabilitate, dezechilibre și surprize strategice, determină schimbări de paradigmă în abordarea conceptelor de lider și leadership militar.

La modul general, liderul militar este persoana vizionară care dispune de pregătirea, experiența, competența și abilitatea de anticipare, inovare, motivare și mobilizare a subordonaților în vederea îndeplinirii unui scop (obiectiv, misiune).

Leadershipul poate fi abordat ca sistem, relație și artă în cadrul organizației militare și presupune abilitatea de a conduce, bazată pe creativitate, inovație, convingeri și motivații, precum și pe capacitatea de a mobiliza și influența subordonații în îndeplinirea unor obiective comune.

Domeniile de valorificare a competențelor liderului militar sunt: conceptual, organizatoric; pregătirea personalului de conducere și instruirea forțelor; integrarea tehnologiilor performante în structura forțelor; susținerea acțiunilor militare.

Rolul leadershipului performant în procesul operației militare vizează planificarea, pregătirea, executarea și evaluarea acesteia.

Pentru prevenirea și contracararea crizelor și conflictelor potențiale din mediul operațional multidimensional este nevoie de lideri militari vizionari, creativi și competenți, precum și de un leadership performant, orientat către oportunități.

Cuvinte cheie: lider militar, cultură organizațională, leadership vizionar, leadership participativ, leadership orientat către oportunități, procesul operației militare.

Abstract: The current security environment, which is multidimensional, high-tech, interconnected and interdependent, is marked by diffuse threats that generate instability, imbalances and strategic surprises which generate paradigm shifts in approaching the concepts of leader and military leadership.

Generally speaking, the military leader is a visionary person, who has the training, experience, competence and ability to anticipate, innovate, motivate and mobilize subordinates in order to achieve a goal (objective, mission).

Leadership can be approached as a system, relationship and art within the military organization and involves the ability to lead, based on creativity, innovation,

beliefs and motivations, as well as on the ability to mobilize and influence subordinates in achieving common goals.

The domains of valorization of the competences of the military leader are conceptual and organizational involving the training of the management personnel and the training of forces, integrating high-performance technologies into the force structure, supporting military actions.

The role of effective leadership in the process of military operation is aimed at its planning, preparation, execution and evaluation.

In order to prevent and counteract potential crises and conflicts in the multidimensional operational environment, visionary, creative and competent military leaders as well as high performance-oriented leadership are needed.

Keywords: *military leader, organizational culture, visionary leadership, participatory leadership, opportunity-oriented leadership, military operation process.*

Theoretical background

The current security environment which is, multidimensional, highly technologized, interconnected and interdependent, marked by diffuse threats generating instability, unbalances, and strategic surprises, determines paradigm changes in approaching the concepts of military leader and leadership.

In this context, acknowledging and understanding the complexity of the security environment as well as the necessity of turning relativism into opportunity within the decision-making process demand a pragmatic approach of the process of training, preparing and developing a new generation of military leaders that are visionary, competent, and motivated, capable of conducting a high quality leadership in the whole spectrum of potential crises and conflicts.

The attitudes, aptitudes, skills and competences of the military leader can reach their full potential only within an organization (military structures) that has the respective culture which describes the character of a group of people, their way of thinking and acting[1].

Thus, organizational culture needs to be regarded as a system of interactions and inter-human behaviors, based on communication, trust, and

---

[1] Simon Sinek, *Liderii mănâncă ultimii: de ce unele echipe lucrează bine împreună, iar altele nu,* Editura Publică, Ediția a 2-a Rev, București, 2017, p. 207.

cooperation, where the military leader motivates and influences subordinates in order to achieve his vision.

In this regard, we might say, generally speaking, that the *military leader* is the person who has the adequate training, experience, and capacity of anticipation, innovation, motivation, and mobilization of subordinates in order to accomplish a goal (objective, mission).

In this restricted sense, the military leader is the person who acts pro-actively in all situations, has the ability to create a vision and the capacity to motivate and inspire subordinates in materializing it.

This requires the leader to show empathy, trust, and responsibility in relation to the subordinates in order to achieve his vision, thus contributing to the development of a credible culture within the military organization. The leader's attitude in inter-human relationships is potentiated by the personal prestige that he/she disposes of within and outside the organization[2].

Military leaders need to have the capacity to work in teams and harmonize their interests, to take on risks and act responsibly in all situations, to admit the value of others and stimulate their initiative. In this regard, the leader has to have the necessary aptitudes and competences for understanding, anticipating, and visualizing the actions of the military organization in order to manage the new challenges existing in the operational environment.

Thus, it can be inferred that the essence of the leader's activities and actions is based on generating the necessary conditions, at decisional, human, and technical levels, that might guarantee the success of the military organization in accomplishing missions, creating the desired effects and the goals set.

At present, the emergence of sudden, unanticipated mutations in the security environment, as well as the development of the information and cyber components, produce transformations upon the military leader regarding the acknowledgment and application of modern leadership methods within the decision-making process.

Leadership is the ability to lead or the art of leadership, based on convictions and motivations, as well as the capacity to mobilize

---

[2] Gustave Le Bon, *Psihologia mulţimilor,* Editura Anima, Bucureşti, 1937, p. 77.

subordinates in conducting a certain task. In this sense, leadership generates change through creativity and innovation, being exerted in a motivated group that accepts accomplishing common objectives.

Leadership may be approached in three hypostases: *process; relationship; art.*

First of all, leadership is a *process* through which a person can influence a group of individuals in pursuing a common goal[3].

Leadership is the capacity of determining the people within an organization to act, being in direct relationship with the capacity of influencing people's behavior[4].

Secondly, leadership is a *relationship* between a leader and his subordinates, characterized by mutual trust and manifested by his capacity to coagulate and mobilize energies around a collective action[5].

Thirdly, leadership is an *art* based on science, which generates modern leadership styles and comprises principles, methods and specific procedure which work together with the leader's abilities based on vision, creativity, charisma, prestige, verbal communication and openness.

From all the theories and models approached in the literature in the field, we are going to refer to the following models of military leadership: transformational; value-based; visionary; participative; digital; opportunity-oriented.

Transformational military leadership presupposes a high degree of motivation of subordinates, based on inspiration, stimulation, and understanding of human behavior, to the purpose of accomplishing with maximal efficiency some common objectives[6].

In this respect, the qualities of military leader, based on charisma, motivation, intellectual stimulation and individual prestige, corroborated with the level of organizational culture, generates a reliable transformational leadership, oriented towards creating a vision that is accepted and achieved by subordinates.

---

[3] *http://onisimbn.ro/sinoiputem/assets/rolul-leadershipului.pdf,* accessed on 12.03.2020.
[4] *Ibidem.*
[5] *buzdugan.com.ro/blogmanagement/?p=2172,* accessed on 03.03.2020.
[6] Dr. Constantin Moştoflei, dr. Petre Duţu, *Liderul militar în România,* Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I", 2007, pp. 38-39.

Value-based military leadership has to do with observing laws, principles, interests, and aims regulating the activities conducted within and by Romanian Armed Forces. Thus, the values that need to be abided are responsibility, capacity of integration in the military environment and adjustment to risks, threats and vulnerabilities[7]. That is why value-based military leadership presupposes a high degree of cohesion in the organization, a flawless behavior, respecting the specific ethics and preserving the security interests in all situations.

Visionary military leadership motivates and persuades subordinates to participate actively at following common principles and ideals. This kind of leadership relies on vision, motivation, and personal dynamism of the leader. At the same time, visionary military leadership is based on strategic and systemic thinking, multilateral vision, collaboration spirit, adaptability, and self-awareness[8]. Only by possessing these characteristics does visionary military leadership acquire coherence in elaborating documents that include scenario and working hypotheses that anticipate specific phenomena and determine their tendencies and perspectives of evolution.

Participative military leadership presupposes the involvement – to a higher or lower extent – of subordinates in making decisions. As a rule, military leaders ensure participative leadership through consulting subordinates and taking into consideration their opinions in the operation-planning process. Moreover, this type of leadership also presupposes the participation of organization members to the decision-making process by consulting them and accepting their ideas and expertise[9]. Thus, teamwork in commands, compartment estimates during the different planning stages, formulating courses of action that are assessed and compared, proposing the course of action that fulfills the conditions considered as optimal for commander's decision, they are all elements of a participative military leadership. Furthermore, participative military leadership also aims at delegating certain duties and responsibilities to subordinates on short, medium, or long term.

---

[7] Dr. Constantin Moştoflei, dr. Petre Duţu, *Op.cit.*, pp. 40-41.

[8] *https://leaders.ro/modelul-de-leadership/,* accessed on 12.03.2020.

[9] *https://virtualboard.ro/teorii-de-leadership-participatil-situational/,* accessed on 12.03.2020.

Military leadership in the digital area has to do with the unprecedented development of information and cyber technologies, integrated and inter-connected within military structures. In this regard, the digital era creates new models of leadership based on innovation, capacity of analysis, originality, vision, power of decision, communication, intuition, and responsibility.

Opportunity-oriented military leadership is the corollary of the other types of leadership, as it presupposes the development of abilities of adjustment to the security environment, anticipation and prediction of military phenomena evolution.

Thus, military leadership needs to apply a correct diagnosis to the respective phenomenon, identify threats and vulnerabilities, anticipate and determine tendencies of evolution and, on this basis, formulate response options that might be credible, flexible, and opportune. Opportunity-oriented leadership stimulates performance and develops the culture of the military organization[10].

That is why we consider that the opportunity-based leadership is the most flexible type of leadership, perfectly adaptable, resilient and efficient in the art of leadership, operational planning, and decision-making.

These theoretical approaches represent the motivation for evaluating the domains of valorizing the military leader's competences and the role of leadership in the military operation process.

Domains of valorizing the military leader's competences

Military leaders show their degree of competence depending on the place they occupy in the defense system, at strategic, operational, or tactical level.

Thus, in the following lines, we are going to detail the domains of valorizing the military leader's competences at strategic level, in order to identify and develop the concepts defining national defense and security.

The modality in which the competence domains of the strategic-level military leader are going to be valorized is based on the following logical

---

[10] *https://www.srac.ro/ro/stiri/semnificatia-rolul-si-importanta-leadership-ului-cadrul-noilor-standarde-pentru-sistemele-de,* accesat la data de 12.03.2020.

pattern: competent leader – motivated and mobilized people – using information and cyber technology – exploiting the characteristics of weapon systems and modern military equipment – efficient leadership – missions accomplished – goals achieved.

In this context, we are going to synthetically refer to the domains of valorizing the competences of the military leader in order to increase resilience in the conduct of a high quality leadership able to ensure the development of the defense system.

The domains in which the military leader is prepared for valorizing the competences acquired are: *conceptual; organizational; preparing the staff and force training; integrating high technologies in the force structure; supporting military actions*[11].

At *conceptual level,* the military leader takes part in developing, harmonizing, and adapting the normative framework to the realities and needs of the military body, given the circumstances of a fluid, uncertain, and unpredictable environment. At the same time, a leader with experience, vision, imagination and initiative understands the imperatives of the moment regarding the development of specific concepts in countering the new forms of conflict (unconventional, asymmetric, non-kinetic and hybrid).

Another significant element refers to the leader's capacity to develop the process of implementation of NATO standards in own structures and participation in ensuring interoperability in military actions.

In order to elaborate a credible concept in the defense domain, the visionary military leader identifies the relations established between threats and response options, between using soft or hard means, between understanding the multidimensional operational environment and the capabilities necessary to shaping the battlespace, force design and engagement.

In this sense, through his capacity of thinking and reflection, the military leader valorizes his experience, vision, and creativity in identifying the opportunities capable of leading to elaborating intelligent strategies and innovative military doctrines.

---

[11] *Strategia militară a României,* București, 2016, pp. 9-10.

These institutional documents support the leader in identifying priorities, establishing goals, motivating subordinates and anticipating the evolution of the military phenomenon in order to participate in elaborating strategic scenarios and hypotheses through which the necessary capabilities are established and the courses of action of forces are developed for different operational situations.

The strategic scenarios and hypotheses require from the leader forethought, analysis and responsibility in orienting subordinates in order to elaborate the operational plans for using force in military actions.

An important role of the military leader can be seen in the way he manages to motivate the team of specialists in understanding his intent and vision, in order to elaborate contingency and military-strategic plans.

The contingency plan is based on hypothetical situations in the area of strategic interest, being developed at a sufficient level that might allow the assessment of the anticipated operation type and identify the nature and dimension of necessary capabilities.

The military-strategic plan is meant to manage a possible crisis at national or NATO level, through the intervention of the forces destined for national or collective defense.

This pragmatic approach allows for the view according to which the leader is a creator of operational added value and, in turn, a creator of other leaders, capable to understand and develop the military domain at conceptual level[12].

At *organizational level,* the leader can valorize his competences through creative and innovative involvement in developing and perfecting the force structure, relying on the principles stipulated in institutional documents that reflect the defense concept in national and multinational context.

Thus, we may say that the military leader needs to have vision, organizational competence, and the ability to create a team in order to coordinate using scientific methods of designing, developing, and perfecting force structures[13].

---

[12] *https://www. danieltanase.com/lider/,* accesat la data de 12.03.2020.
[13] *http://mihaicurteanu.blogspot.com/2014/09/ce-inseamna-leadership-si-care-sunt-calita-tile-unui-leader.html,* accessed on 12.03.2020.

In this sense, the visionary military leader, who has the necessary abilities for motivating and inspiring subordinates, may conceive the organizational architecture of the force structure in the following mixed manner: *on the basis of risks, threats, and vulnerabilities; function of capabilities; oriented towards opportunities.*

In the first category, the force structures should be conceived, dimensioned and developed in order to efficiently respond to the whole range of threats in the security environment.

The ability of the military leader to lead the team in designing the force structure which might efficiently respond to threats consists in his capacity to identify the tendencies and evolutions of the security environment in order to sense the situations in which sudden and unanticipated changes may occur, generating strategic surprises.

In this sense, the military leader directs the team towards projecting some *core structures* which might be completed in case of sudden threats, so as to avoid the occurrence of strategic surprises.

Regarding the second category, force structures should be conceived, dimensioned, and developed as such so as to ensure the capabilities necessary for managing and solutioning any situations with risk potential which might create vulnerabilities in the security environment.

In this context, the military leader directs the team in the sense of identifying and projecting those capabilities which might integrate the forces and means necessary to conducting the entire spectrum of military operations.

In the third category, force structures need to be conceived, designed, and developed on the basis of being opportunity oriented. In this regard, the military leader identifies the opportunities in the security environment, establishes priorities, anticipates tendencies and directs the team towards designing some force structures that are mobile, flexible, and adapted, capable of offering an efficient response to potential crises and conflicts.

Moreover, identifying opportunities offer the motivation of establishing *task forces* meant to participate in multinational operations in allied context or within some coalitions.

Regarding the *training of the command staff and force preparedness,* the military leader valorizes his experience, knowledge, and competences in order to think over and implement documents regarding the training of the

forces in Romanian Armed Forces, in accordance with NATO provisions in the field. In this sense, the visionary military leader directs the team so as to elaborate a multiannual training program for the command staff and force preparedness so as, on medium term, to conduct the entire range of exercises in the extended operational environment, in national and multinational context.

Taking into account the new forms of manifestation of conflicts, the military leader identifies priorities and opportunities for training command staff and forces, emphasizing the conduct of complex, joint, integrates and multinational exercises in an extended operational environment.

Depending on the typology of the strategic scenarios and hypotheses elaborated, the military leader directs the team in planning exercises that have the purpose of assessing the capacity of commands and the level of force training in unconventional, asymmetric, non-kinetic and hybrid operations.

At the same time, the military leader valorizes his abilities and competences in the manner in which he motivates, convinces, and influences the activity of the team in elaborating the documents for carrying out exercises and ensuring their efficient conduct in order to fulfill their missions and accomplishing the respective purposes by the structures involved.

Taking into account the importance given to training through simulation, the military leader needs to be trained to use experience in a creative manner in planning, preparing, and conducting this type of exercises in various operational situations, with the designated force structures.

Upon finalizing a cycle of training for command staff and forces, the military leader needs to have the ability and competence to identify and valorize the lessons learned resulting from the conduct of exercises at national and multinational level.

Regarding the *integration of high quality technologies in the force structures,* the military leader has to have the necessary knowledge and competences for directing subordinates in understanding the place and role of modern systems and armaments and information infrastructure within the military organization, as well as the manner to exploit them for obtaining success in mission accomplishment.

In this sense, the leader valorizes his abilities and professional competences in motivating subordinates for understanding the advantages of integrating modern technologies within the force structure and developing their skills to exploit them adequately, thus ensuring the necessary conditions for obtaining information, decisional, and action superiority in the efficient conduct of military actions.

An important issue that needs to always be subject to attention of military leader refers to the manner in which command and control systems through integrating and inter-connecting information technology, which might ensure the conduct of a collaborative, opportune, and credible decision-making process.

Regarding *sustaining military actions,* the leader needs to be permanently concerned with improving the endowment of the force structure with weapon systems, fight technique, and high-quality materiel. In addition, he has to understand the necessity to purchase and endow forces with armament and compatible military equipment, interoperable with those used within NATO, in order to conduct common exercises and combat missions, in a multinational context.

A competent and responsible military leader makes operational requirements, raises awareness and persuades his subordinates to act in order to purchase and endow the force structure with efficient military systems and equipment, as well as with information technologies that might ensure the successful accomplishment of missions at national and multinational level.

The role of leadership in the military operation
Leadership means creativity and innovation, as well as the capability of leading a force structure through vision, conviction, and influence in order to reach a common goal.

At the same time, leadership is the art of leading people by using conviction methods consisting of non-coercive means, having as a final goal the fulfillment of the commonly established goals.

What results is a combination of leadership styles for a particular task force, using a visionary, participative, and opportunity-oriented leadership.

In this context, we need to mention the important role played by leadership in the process of military operation consisting of *planning, preparing, conducting, and evaluating it[14]*.

Operational planning is a complex process which, in order to be successful, should include visionary, opportunity-oriented leadership, based on the leader's capacity to motivate and determine people to act and on the ability to influence the behavior of the command staff in order to make an efficient decision and elaborate a credible operation plan/order.

At the same time, operational planning presupposes a participative leadership, as the leader consults and involves the entire command staff in each phase of the process, having as concrete end-state decision-making and elaborating the concept of operation and the operation plan.

Applying a leadership style which aims at being appropriate and successful presupposes the existence of a strategic culture within the command, shaped in time, requiring knowledge, experience, understanding, and innovative thinking, great team spirit, IT and cyber working skills and competences.

A kind of leadership that is visionary in planning presupposes integrating and inter-connecting the instruments and mechanisms of analysis in order to establish an optimal ratio between diagnosis and prognosis, between vulnerability and opportunity, as well as between the leader's responsibilities and the duties delegated within the command's compartments.

If diagnosis refers to acknowledging the real situation by determining the identity of the respective phenomenon, prognosis presupposes anticipating and evaluating its tendencies of evolution and perspectives of development.

Vulnerabilities are consequences of certain dysfunctionalities of deficiencies which might diminish the efficiency of the command and control system and may create the conditions for risks and threats impacting the force structure.

Opportunities refer to the successful elements identified in the operational environment which, if judiciously exploited, may mitigate the vulnerabilities and potentiate the activities necessary for making an efficient

---

[14] S.M.G.-3, *Manualul de planificare a operațiilor,* București, 2016, p. 31.

decision which, in turn, is going to create optimal conditions for own actions and ensure the expected effects, the fulfillment of objectives and the achievement of the desired end-state.

In this regard, a kind of visionary leadership identifies the existing vulnerabilities within the own system and the operational environment, determines opportunities, establishes the necessary force structure and formulates response options for countering the threat.

Regarding the leader's responsibilities and delegating duties as a type of participative leadership, we consider that there should be a balance between the minimal limit involving consultation and the maximal limit consisting in embracing the command staff expertise, so that the leader may benefit from the subordinates' estimations and propositions but, at the same time, he may take full responsibility and assume the authority of decision-making.

A high-quality leadership aims at motivating and stimulating the command staff both horizontally, within the command, in order to carry out an efficient activity, and vertically, by developing the trust, abilities, and competences of subordinates, using as a procedure the collaborative planning, meant to shorten the length of the decision-making process and elaborating command documents at multi-echelon level.

The preparation of the military operation is a coordinated process within which leadership has an important role in the short-time accomplishment of the fight capacity of the force in order to fulfill the objectives set in the action plan. In this respect, leadership addresses directly the force structure through the capacity of the leader to communicate, motivate, and mobilize subordinates in order to successfully accomplish the missions received.

At the same time, preparing the military operation presupposes applying a participative leadership within which the leader coordinates the training activities. The people within the command staff who have received tasks through delegating responsibility ensures the conduct of training according to the plan, while subordinates act for the cooperation of forces and synchronization of missions.

In this stage, leadership aims at conducting activities able to ensure the efficient use of combat power by executing repetitions, organizing and shaping the force for accomplishing the mission received, instructing,

training and transmitting tasks towards subordinates and checking the means of understanding their content.

The role of leadership in executing repetitions refers to stimulating, determining, and mobilizing the force for exercising those procedures that potentiate the action and make it more dynamic. Thus, repetitions reflect the leaders' capacity and ability to direct actions towards neutralizing the enemy's center of gravity, in order to accomplish the effects established and fulfill the objectives specified through the mission. In addition, applying a high-quality leadership during the repetitions, based on communication skills, integration, coordination and synchronization of actions of the force, ensures the indicators necessary to achieving the combat power which might allow surprising the enemy and potentiating the execution of missions.

Organizing and shaping force for accomplishing the mission received implies a participative leadership oriented towards the need of ensuring the necessary resources. In this sense, efficient leadership presupposes conducting, coordinating, and stimulating some actions through which organizing the force for mission might be correctly dimensioned in relation to the effects and objectives established.

This correlative approach of the relation between dimensions of the force task and the amplitude of the mission has to do with applying an efficient leadership capable of offering the necessary conditions for success in the military operation.

Training subordinates is a long-lasting process that takes place before the military operation planning but intensifies during the preparation phase.

In this phase, leadership directs the training and instruction of the force towards coordinating, cooperating, and synchronizing the action of force components in order to apply the combat power in a synergic manner.

Thus, we have to underline the role of leadership in the ability and capacity to mobilize, convince, and encourage personnel to put together exercises that reflect the physical or virtual operational environment, to allow the identification of opportunities and synchronized action of the force for accomplishing the mission.

At the same time, a visionary leadership presupposes motivating and convincing the force to execute training and instruction activities as closely to reality as possible, to practice the adequate maneuver types, to

synchronize the actions of the striking system, to achieve multidimensional protection and joint logistics.

Conveying the missions to subordinates and checking the manner of understanding their content are based on the action plan elaborated within the command.

In order to check the manner of understanding the missions received by subordinates, leadership has to prompt the elaboration of a control plan adequate to the leader's demands.

Execution of the military operation is the culminating point of the confrontation, when all physical, cognitive, and moral energies act in a synergic manner to obtain success.[15]

In this regard, leadership aims at mobilizing the force, exploiting opportunities, sustaining morale, encouraging subordinates and making them feel responsible for applying the operation plan for engaging the enemy and accomplishing the missions received.

In this stage, leadership supports the execution of the operation through initiative, dynamism, flexibility, and ingenuity in thinking and acting. Furthermore, visionary leadership should identify right on time the threats that can make the mission of own forces vulnerable, act in order to reduce them, and exploit the opportunities that ensure success.

Thus, we may say that the role of leadership in the dynamics of operation becomes very important as it mobilizes, encourages, and potentiates the permanent coordination and synchronization of the force in executing the missions and establishing the objectives established.

The ability and capability of permanent adaptation of the fight procedures to the concrete situation, the reduction of the effects of desynchronization, the valorizing of significant information and action flexibility are conditions for success generated by the application of a visionary type of leadership.

At the same time, an efficient leadership aims at directing the subordinates towards respecting the maneuver scheme, engaging the significant enemy targets, maintaining force protection and viability of logistic support.

---

[15] S.M.G.-3, *Manualul de planificare a operațiilor,* București, 2016, pp. 80-81.

In this sense, leadership requires creativity and innovation in the advantageous layout of the force that might allow it to perform the dominant maneuver so as the enemy be taken by surprise and overwhelmed, and the objectives be rapidly conquered.

At the same time, leadership has to support and sustain the concentration of effort on the essential elements of the mission converging towards the enemy's center of gravity, as its annihilation only is what ensures the success of the military operation.

The change of operational situation during mission execution requires from leadership the conduct of different activities for adjusting the plan and the elaboration of new fragmentary orders so as actions might have continuity, the combat formation might maintain its dynamism and speed and the pace of actions be in accordance and the rhythm to be constant and in accordance with the goals set.

The capacity of anticipation, experience and critical thinking facilitate the adjustment of the force to the new situations occurring on the battlefield without having to execute certain maneuvers and ample or complicated re-positionings, without substantially changing the goals set initially.

All these conditions of success cannot be accomplished without a visionary leadership that is both participative and opportunity-oriented, able to valorize the information and information products in the area of interest, obtain information superiority, and sustain the potentiation of actions in the whole spectrum of the military operation.

The assessment or evaluation of the military operation is the process through which leadership checks the manner of accomplishing the missions and the concordance between the content of the plan and the level of execution of actions in the battlespace[16].

Thus, we emphasize the extremely important role the leader plays in the assessment of the operation, as the results obtained from this action can prove useful for the planning of future actions, eliminating as much as possible the lacks of agreement, the overlapping, the desynchronizations and dysfunctionalities in executing the missions by the task force.

---

[16] S.M.G.-3, *Manualul de planificare a operațiilor,* București, 2016, p. 166.

In fact, in the process of operational assessment, leadership ensures the feedback between the action plan and the manner in which the mission was accomplished, offering a set of lessons learned that will be valorized in planning the future military operation.

The leader has the role to coordinate and direct the command staff in order to constitute a specialized structure able to quantify the consequences and the effects of actions undertaken in the area of operations.

In this regard, leadership determines and directs the appointed people towards establishing the efficiency and performance indicators measuring the results obtained during the carrying out of the actions, in relation to the content of the plan, the degree of achievement of effects and objectives initially established.

Also, setting the assessment indicators of the military operation has to do with a leadership based on opportunities, characterized by agility, flexibility, and creativity, in order to efficiently measure the efficiency and performance of force structures during mission execution.

Furthermore, opportunity-oriented leadership needs to assure the optimization of the process of military operation assessment by using relevant criteria and the resulting products should determine real feedback, conducive to improvement of the activity of command staff within the HQ in planning future actions.

Conclusions

The dynamic, fluid, and unstable security environment, generating diffuse threats, situations that change suddenly and unexpectedly as well as strategic surprises causes changes of paradigm in approaching the concepts of leader, leadership, and military organization.

The military leader has prestige, intellectual capacity, motivational ability and professional competence of anticipation, innovation, and mobilization of the members of an organization in order to accomplish a goal.

In this respect, the leader is endowed with vision, he thinks synthetically and proactively, shows empathy, motivates and influences his subordinates without using coercive methods and has the ability to develop the capacity of the personnel within the organization to materialize his concept for achieving the established aims.

That is why it is said that the leader is the person who has abilities, experience, character, and loyalty for and to the organization and engages his team in accomplishing his vision.

Leadership approached as an interhuman system, as a relationship between the one who is leading and those who accept being led, and as an art of leading requires from the leader creativity, vision, innovation, conviction, and motivation, as well as the capacity to mobilize and influence subordinates in accomplishing some common goals.

If the most important feature of the military leader is his capacity to motivate and mobilize the participants in some activities, the most important feature of leadership means hierarchy, creativity, and innovation in the management of an organization.

As a corollary of leadership styles, we might say that opportunity-oriented leadership corresponds best to diagnosing the current security environment, to identifying threats and vulnerabilities, to diminishing dysfunctionalities and uncertainties and providing inter-institutional response options that are flexible, credible, and efficient.

Given the complexity of the security environment and the multitude of component elements, the application of a high-quality leadership in the military operation process constitutes the guarantee for success in accomplishing missions.

In the end, we may say that the complex nature of the topic approached should lead to revisions and redefinitions and rethinking concepts in the changing paradigm and new principles should be applied in order to develop and perfect the competence of leadership and its role in the military operation.

References

1. * * *   *Strategia Militară a României,* Bucureşti, 2016.
2. * * *   S.M.G.-3, *Manualul de planificare a operaţiilor*, Bucureşti, 2016.
3. Dr. Constantin, Moştoflei, dr. Petre, Duţu   *Liderul militar în România,* - Bucureşti: Editura Universităţii Naţionale de Apărare „Carol I", 2007.

4.	Gustave, Le Bon	*Psihologia mulțimilor,* Editura Anima, București, 1937.
5.	Simon, Sinek	*Liderii mănâncă ultimii: de ce unele echipe lucrează bine împreună, iar altele nu,* Editura Publica, Ediția a 2-a Rev, București, 2017.
6.	* * *	buzdugan.com.ro/blogmanagement/?p=2172
7.	* * *	http://onisimbn.ro/sinoiputem/assets/rolul-leadershipului.pdf
8.	* * *	https://leaders.ro/modelul-de-leadership/
9.	* * *	https://danieltanase.com/lider/
10.	* * *	http://mihaicurteanu.blogspot.com/2014/09/ce-inseamna-leadership-si-care-sunt-calitatile-unui-leader.html
11.	* * *	https://virtualboard.ro/teorii-de-leadership-participatil-situational/
12.	* * *	https://www.srac.ro/ro/stiri/semnificatia-rolul-si-importanta-leadership-ului-cadrul-noilor-standarde-pentru-sistemele-de

SCHIMBĂRI ALE PARADIGMEI STRATEGICE GLOBALE ÎN URMA BREXITULUI

THE SHIFT OF THE GLOBAL STRATEGIC PARADIGM FOLLOWING BREXIT

Professor Costel DUMITRESCU, PhD
Tenured member of the Academy of National Security Sciences,
E-mail: dumitrescucostel1@gmail.com
.

Rezumat: Numărătoarea inversă a început. Uniunea Europeană este la răscruce de drumuri, deoarece Marea Britanie a părăsit UE. Marea Britanie și UE nu au ajuns la un acord privind condițiile de ieșire și, de preferință, un nou acord comercial. Ambele părți au parcurs un drum imprevizibil. În ciuda faptului că principalul nostru scenariu era ieșirea Marii Britanii din UE la 31 octombrie 2019, acest lucru s-a realizat la data de 31 ianuarie 2020. Începând cu această dată, Regatul Unit a putut începe eliminarea sau introducerea legilor UE, dacă se dorește.
Cuvinte cheie: peisaj politic; nivel de trai; șomaj; criză; piață comună; potențial economic; echilibru; impact financiar.

Abstract: The countdown has started. The European Union is right at the crossroads, as Great Britain has left the EU. Great Britain and the EU have neither reached an agreement regarding the conditions for exit nor signed a new commercial deal as it would have been preferable. Both parties involved have followed an unpredictable pathway. Despite the fact that the main scenario anticipated the exit of Great Britain from the EU on October 31st 2019, this was accomplished on January 31st, 2020. Starting with that date, the United Kingdom was free to start eliminating or introducing EU laws according to its interests.
Keywords: political landscape; standard of living; unemployment; crisis; common market; economic potential; balance; financial impact.

Introduction

Brexit is a historical turning point whose roots go far, over 70 years in the past. Also, its consequences are going to have long-term effects. England's decision to launch Brexit did not erase the topic debated within the EU, but rather created new controversies and divided the country in sides proving to be farther than ever from the idea of reconciliation. The

presupposed benefits brought by Brexit still remain vague; yet, its economic problems are concrete. In turn, the EU is currently dealing with an existential crisis.

According to an insider's opinion (somebody who knows about this domain)[17], the myth of irreversibility and the claim to embody the manifest destiny of Europe have vanished. The EU is losing an important, efficient, and economically powerful member.

The author, who worked as a diplomat at Germany's Embassy in London, shows in this book how the referendum for Brexit could take place and how the result could be evaluated. Which are the approaches followed by Theresa May with its cabinet in order to implement voter's decision? Which are the perspectives for the future for the United Kingdom? Which may be the consequences of this loss for the entire EU and especially for Germany?

The answers to these questions represent the starting points for the captivating and vivid analyses and diagnoses made by this author, as well as by many contemporary political analysts.

Great Britain referendum regarding leaving the European Union generated a lot of reviews, articles, editorial opinions inter pares. All these positions are convergent in a single direction – Great Britain and the EU have entered an unpredictable dynamics and have added an entire series of new variables, though still confusing, for the situation which is already troublesome in Europe and in the world.

In the experts' community, a relative consensus has developed, regarding the prognoses of development for events which are presumably going to be the following: the more uncertainty is going to persist, the more detrimental are going to be both the direct and the indirect effects upon the integration process as well as upon the global market. At the same time, Brexit has created a new, unexpected reality, in which it is possible to witness a change of roles in some states' regional and global actions, including Russia and the states between Russia and the EU.

---

[17] Rudolf G. Adam, *BREXIT: Eine Bilanz,* Publisher: Springer Fachmedien Wiesbaden, Year: 2019. *N.a.* The author who worked as a diplomat at Germany's Embassy in London talks in this book about how Brexit referendum could take place and how the result should be evaluated.

Opinions regarding Brexit

At first sight, the referendum has become a combination of short-term political calculus, created for attracting the public opinion, whose influence upon the political dynamics has been underestimated once again. Similarly, rational arguments in favor of the benefits of integration, free circulation of people, capital, and services in Europe were not sufficient for overcoming the balance in favor of the supporters advocating EU membership.

Discourses on Brexit offer a vast array of perspectives about the way in which they influenced the result of this European social-political result.

Working with an ample amount of data, from political discourses up to Twitter posts and a significant amount of methods, the authors of *Discourses of Brexit*[18] present the most detailed exam of discourses around the British referendum, the EU, and the connected events.

The analysis of these discourses offer a comprehensive understanding of Brexit's discursive treatment, at the same time offering detailed investigations about the way Brexit was negotiated in different contexts, both for the experts in geopolitics and for everyone interested in developing their understanding of the referendum.

The referendum played an important role – it finally approved the arguments long made by Euroskeptics in the political mainstream which, until recently, seemed to become marginal as it did not manage to cast a serious shadow on the European way of the Brits.

However, the cautious attitude regarding European institutions is not a slogan for Great Britain; it exists just as long as the idea of a united Europe exists and it is not the first time it has emerged, especially during electoral campaigns. Furthermore, forcing Euro-skeptical ideas has not always fallen upon the Conservative Party.

At the beginning of the'80s, Great Britain's exiting the European Economic Community was one of the points on the political agenda of the Labour Party, but they were compelled to abandon it after a resounding defeat in 1983 due to the Conservatives led by the „Euro-skeptical

---

[18] Veronika Koller, Susanne Kopf, Marlene Miglbauer, *Discourses of Brexit,* Publisher: Routledge, Year: 2019.

progressist" Margaret Thatcher. Moreover, the Conservative government, led by Harold Macmillan, took historical steps towards the European integration in the '60s, so as the preferences of the party in this case did not have clear patterns.

After the Maastricht Treaty entered in effect in 1993, the leading parties pleaded for continuing European integration, preferring to moderate criticism towards Brussels and seeking for special conditions for London. Although among the conservatives at the beginning of years 2000 there were attempts of getting closer to continental Euroskeptics, they were supported neither by the leaders nor the majority of the party (including David Cameron).

The only political force that not only adhered to an open anti-European policy, but it also built its program around it was the UK Independence Party (UKIP). It was founded in 1991 by a series of intellectuals – university professors and public figures – who opposed Maastricht Treaty. For fifteen years, UKIP was on the front pages of mostly tabloid press, drawing little attention from top politicians and serious experts. However, this situation only went on until the leader of the party became Nigel Farage. Together with N. Farage, UKIP made a little revolution in the political landscape apparently stable of Great Britain, succeeding in attracting the votes of many people and different social groups as it opposed not only European integration, but also immigration, globalization, trans-national corporations etc.

N. Farage and his associates did not hesitate to use the populist rhetoric, advocating ideas such as restricting migration, re-establishing Great Britain and severing connections with Brussels bureaucrats. They used a set of anti-liberal slogans, against the backdrop of the consequences of the crisis in 2008-2009. They enjoyed increasing popularity in all Europe. UKIP's success (in several electoral campaigns) and the fact that for instance, at the elections for the European Parliament in 2014, it obtained 28%, that was more than the three main British parties, caused turmoil and splits both inside the Conservative and the Labour sides. Consequently, there was a consolidation of both right-wing and left-wing extremist factions' positions, whose representative figures were Boris Johnson and, respectively, Jeremy Corbin.

John F. Kennedy used to say: „*Voters vote for us because they trust our judgement and our capacity of understanding the nation's interests. This means that any time it is possible, we should guide, inform, correct, and sometimes even ignore public opinion*"[19]. The very fact that a referendum was announced regarding the matter of Great Britain exiting the EU was the result of the failure of some moderate British Conservatives led by PM David Cameron. They believed they could simultaneously deal with Euroskeptics in their own party and with that part of the society to whom globalization and integration were synonymous with the failure of British economy and the decline of the nation.

Yet, statistics show that along the years during which Great Britain was part of the , the economic situation of the country did not deteriorate at all: the GDP per inhabitant grew from 5,500 pounds in 1998 to almost 7,000 in 2015, while the number of private companies in 2015 touched a record level of 5.4 million in comparison with 3.5 million in 2000. The rate of unemployment, exceeding the negative context of period 2008–2012, returned in 2014 to a comfortable 6%, which is comparable to the end of the '90s and much better than the strongest fluctuations on the labor market in the interval 1970-1980.

Thanks to British press, a stereotype emerged according to which great companies were in favor of preserving the quality of EU member state, while Brexit was supported by small enterprises, which is not entirely true. If large companies did support almost completely the idea of following on the European path, within the area occupied by small and medium firms and companies was quite divided. Many of their representatives considered European standards as being too complex and pleaded for larger freedom as compared to what was coming from European bureaucrats. However, largely due to European standards, the British economy in the last quarter of the century became more competitive and managed to surpass the effects of the numerous crises and recessions in the years 1970-1980.

Nevertheless, in the end, the confrontation between the supporters of Great Britain staying in the EU and those advocating for Brexit did not turn into a battle of rational arguments, but rather into a natural fight for

---

[19] Kennedy JF, *Profiles in Courage*, Published by Harper & Row, NY, 1956, p. 15.

votes – with massive campaigns of mass manipulations, live performances of politicians and celebrities and colorful shows such as the naval parade on the Thames. Yet, there was a dangerous tendency behind these campaigns – the dependence on the public opinion at a moment when serious and well thought decisions were needed from superior leadership.

It is interesting that among the regions that gave most of the votes for Brexit were England and Wales who had to suffer, objectively speaking, because of the effects of irregular markets and budgetary economies. However, such arguments were hardly used by Brexit critics. On the contrary, their campaign was based on criticism towards European Union and migration as main reasons for decreasing the standards of living and increasing unemployment.

It is obvious that in periods of crisis, the public opinion tends towards simplest and more intelligible answers. Which would be the result of a referendum, for instance in Germany, if there were a vote regarding the issue of financial assistance provided to Greece? What would French citizens recommend if they were asked regarding restrictions on migration coming from Arab countries. The answers are obvious for most countries, but would it be correct – for these countries and for Europe – to ask these questions?

A referendum in Great Britain was an obvious demonstration of the potential of a dysfunctional democracy. They resorted to public voting when actually what would have been needed was a balanced parliamentary procedure, involving active consultations with all the interested groups. The lack of such serious consultations and of a well-documented work in the field led to the situation in which the third European economy did not have a clear action plan in case of withdrawal from the European Union.

Generally speaking, instability is inherent to markets – they answer any international crisis with explosions of volatility. However, Brexit became an unusual crisis for the markets. The willingness of British people to abandon the accepted rules of the game served as a new variable in relation to which markets, including the British one, could no longer develop an unequivocal position. Nowadays, the main economic institutions, states and companies in the world are compelled to work simultaneously with several scenarios – from a positive one to an extremely negative one. The possibility of implementing these scenarios depends on a

series of factors that are mainly associated with the speed and efficiency of finding a new status-quo between London and Brussels.

Still, it is obviously premature to say that Brexit is going to cause a new global economic crisis.

Some economic aspects of Brexit

Catastrophic scenarios are traditionally popular in mass-media, but British economy has an enormous safety margin. This has been confirmed by the strengthening of the pound and a visible decrease of the panic on the stock markets in the first weeks after the shock of referendum results. IMF decreased, it is true, the prognosis of global economic growth for 2017 by 0.1%, and for Euro zone with cu 0.2% . However, these calculations are still quite speculative in nature as everything is going to depend on the same scenarios and negotiations with Brussels. Also, it is now impossible to predict how much the consequences of Brexit are going to account for in the British economy. The financial research institute in London, one month prior to the vote, established a range between 74 billion pounds and a surplus of 30 billion pounds, function of the evolution of the situation. Figures are so diverse than no serious economist could name even the approximate cost of Brexit.

Despite this fact, the Euro zone is nowadays experiencing more distinctive risks associated to the state of uncertainty of the financial sector in Italy and the hazardous operations form Deutsche Bank. In case of negative scenarios for the Italian and German banking systems, they will have a much more rapid effect upon European economy. The structural issues of high unemployment, low productivity and low dynamics of credits has not disappeared. Brexit only added the economic uncertainty in the region, which might increase the burden on the financial sector. European Union, that missed British investments in its budget (approximately 15 million pounds per year), is going to have to compensate for them to the detriment of other member countries, first and foremost Germany.

Those who see the break-up with Brussels outside the European Union as a well-thought strategy consider that Great Britain is going to be exempt for the burden of systemic issues in continental Europe and is going to be able to improve economy in an independent manner. The main vulnerability of this position is that independence in the modern world is a

conditioned category. There are no independent markets for services, financial systems, innovative industry, etc. So, the question is, what part of the new whole is Great Britain willing to become?

The most optimistic scenario described in the Out campaign involves the following: after receiving the right to independently sign commercial agreements, the country will not remain solely in the free exchange zone with the EU (nor will it close separate agreements with it on economic sectors), but will significantly expand its area of influence by creating new economic-financial markets with the main economies of the world – United States, China, India etc. This should turn Great Britain into a unique commercial and financial hub, as a new Switzerland or Singapore. One of the nuances of a possible agreement between London and Brussels is that it is practically impossible to get free access to EU financial markets without being member of the bloc. Especially Switzerland, which has a bigger prevalence of financial services in GDP than Great Britain, has a commercial deficit with the EU regarding financial services – the position of a privileged partner is not yet equivalent with full membership.

The unicity of Great Britain before Brexit was that the country served as a bridge of investments between European Union and the rest of the world. United Kingdom implied more direct investments than the entire EU combined. According to a study made by Ernst & Young in 2015, most investors (72%) declared that the main advantage of United Kingdom is free access on the European market. In other words, investors considered the Island-state not only as an object for investment, but also as a major transit-zone. Supporters of withdrawal from the EU have tried so far to refrain from convincing world investors that this chain is going nowhere in the future.

However, this is going to require closing a unique agreement with Brussels unlike any other in Europe. This should prescribe simultaneously free access on a unique market and restrict the free movement of people (namely, migration) – one of the main points of *Out campaign*. If the victorious faction of Euro-skeptical conservatives and of other socio-political forces that pleaded for withdrawal from the EU abandon this populist point, they are going to lose the support of the "angry" part of the population and are going to choke their own efforts.

In a certain way, this was the most difficult and the true reason for which the negotiation process happened with such difficulty, as Brussels,

Berlin and Paris could not agree that "people" can be eliminated from the free movement. Finally, this will mean a transgression or the necessity to partially revise the Union's legal fundaments.

A few global consequences

For the countries outside the EU and especially for Russia, the short-term consequences of Brexit will most probably be indirect in nature, by fluctuations of raw materials markets and currency fluctuations caused by the uncertainty of subsequent events. Maybe some of the big companies that traditionally make transactions at London Stock Exchange will wish to avoid financial volatility and suspend transactions or sell a part of their actives. At the same time, it should be mentioned that the tendency of former Soviet enterprises to leave London Exchange occurred long before the referendum and was caused by completely different reasons: a global decrease of the price of raw materials, the loss of interest of a number of key-investors in Russian actives against the backdrop of a new round of geopolitical and geoeconomic turbulences and economic stagnation in Russia.

In many aspects, some of these unfavorable factors imposed in 2015 eliminating firms such as Uralkali, Polyus and Eurasia BC. Eventually, some companies acting internally in Russia (for instance, Otkritie Bank) expressed their desire to transfer trade on attractive Asian markets. Still, there is no anticipation of the other Russian companies (31 in number), leaving the Stock Exchange in London as there were a lot of close connections developed in the middle of years 2000 between Russian businessmen and London financial providers. If the interest continues to decrease, the cause seems not to be found in Russia, but with the frustrated foreign investors, and in this case the transfer of trade towards Hong Kong, Shanghai or Singapore is quite unlikely to save these companies from a loss of cash.

A significant number of top western politicians who supported the *In* Campaign, including David Cameron, said that Moscow is going to be the first to benefit from the British exit and from the weakening of the EU. This argument, quite childish from a reasonable point of view, could have been an attempt to give a simple answer to the question why Brexit is bad.

As for extending or gradual elimination of sanctions against Russia, Brexit probably plays a role, but not a decisive one. In reality, its duration is extended by all EU members, unanimously. Even if there is no official vote of the United Kingdom in European institutions, there will be other countries willing to adopt a strict position against Russia; at the same time, the opinions of Great Britain as an important regional actor will clearly not disappear.

Despite this, nowadays, things seem to be going in the opposite direction – more and more important political groups and business representatives in EU member countries declare the necessity of relaxing the sanctions. If these groups gain followers and supporters in the critical mass, especially in the top economies of the Union, then the effect obtained might be exactly the opposite to the one anticipated. Obviously, Great Britain – irrespective of whether has been in the EU or outside it starting with 31st January 2020 – could or would hardly reverse this situation.

The regime of sanctions is, anyway, a temporary phenomenon for Russian-European relations. Another thing is more important – the way in which Russia and the European Union are going to build their strategic relations in the future and the role that Brexit might play in this dynamics. In the latest years, Russia has adopted a rather passive position (depending on the connotation) regarding European integration. The political-military uncertainty, often accompanied by hysteria, does not add rational fundaments for a more profound involvement of Russia.

Obviously, a scenario of unification between Eurasian Union and European Union, which was repeatedly criticized and is still generating intense comments, still has enormous potential, but its application requires political will and serious efforts from experts. Even if nowadays Russian elite has mostly directed its attention towards another union – with the economic belt of the New Silk Road, this does not mean that Russia is going to turn down participation in the western processes of integration.

In this respect, Brexit is creating a new paradigm which has not been disclosed yet. Odd as it may seem, this step which is still obscure and in large measure populist of individual political circles in Great Britain is capable to significantly change the regional space and open up new opportunities, including for Russia and Turkey.

Conclusions

In the context of change of leading elites in Great Britain, the search for new paradigms of development by the European Union, the active interaction of integration projects (transatlantic partnership scenarios), the Russian and Turkish leaderships should not focus on obtaining power influence, but rather Smith's benefit (economic rationalism), this being a new reality.

In a period in which Europe has entered a phase of uncertainty, Moscow should start to study not only the risks but also the potential advantages – regarding the new formats for commercial and financial cooperation with London, opportunities for a constructive reversal in the relationships with the European Union and a reduction of geopolitical tensions. Up to the present, in the analytical environment, there have been only timid attempts to understand the potential of economic closeness to Great Britain, independently of Brussels or the revision of relations with the EU, some of them seeming simple scenarios.

Brexit creates real opportunities, both for Moscow and for Ankara, but not from the point of view of an alleged weakening of the EU that western politicians insist on, but rather from the point of view of reforming the European economic space in which Russia, as a main energetic vector, might develop a participation in favorable conditions both for it and for Europe.

This article approached some of the most important aspects of Brexit that were constantly present in public debates but which, until the present, have not been sufficiently developed by authors in the field.

In order to solve this delay, a work comprising contributions from an international group of authors[20] put together a comprehensive and multidisciplinary perspective upon this topic. More precisely, scientists from Great Britain and the entire Europe offered different accounts related to law, political science, and European studies.

---

[20] Thomas Christiansen, Diane Fromage, *Brexit and Democracy: The Role of Parliaments in the UK and the European Union,* Series: European Administrative Governance, Publisher: Springer International Publishing; Palgrave Macmillan, Year: 2019.

Beyond providing a comprehensive picture of Brexit control, the article uses the ideas derived from these experiences for a study of social-political relations in the European Union, in general, examining the balance or the lack of it precisely between governments and parliaments. Thus, we are left with some of the long-term questions, truly long-lasting, about the effects of constitutional provisions and political practice in the context of European democracy.

References

1.	Rudolf G. Adam	*Brexit: Causes and Consequences,* Publisher: Springer, Year: 2020.
2.	Rudolf G. Adam	*BREXIT: Eine Bilanz,* Publisher: Springer Fachmedien Wiesbaden, Year: 2019.
3.	Thomas Christiansen, Diane Fromage	*Brexit and Democracy: The Role of Parliaments in the UK and the European Union,* Series: European Administrative Governance, Publisher: Springer International Publishing; Palgrave Macmillan, Year: 2019.
4.	Duță, Paul	*Europa lărgită, politica europeană de vecinătate și spațiul comun de securitate externă*, în Impact Strategic, nr.2/2005.
5.	Duță, Paul; Grațian, Lupu	*Europa de la dezideratul unificării la OSCE și Uniune*, Colecția Politică și Apărare Națională nr. 11, Editura Continent, Sibiu, 2006.
6.	Kennedy JF	*Profiles in Courage,* Published by Harper & Row, NY, 1956.
7.	Veronika Koller, Susanne Kopf, Marlene Miglbauer	*Discourses Of Brexit,* Publisher: Routledge, Year: 2019.

PANDEMIA DE CORONAVIRUS – RISC SAU AMENINŢARE LA ADRESA SECURITĂŢII NAŢIONALE, REGIONALE ȘI GLOBALE?

CORONAVIRUS PANDEMIC – RISK OR THREAT TO NATIONAL, REGIONAL AND GLOBAL SECURITY?

Major General (ret.) Professor Gabriel-Florin MOISESCU, PhD
Tenured memeber of the Academy of National Security Sciences,
E-mail: moisescu.gbrl@gmail.com

Lieutenant Colonel, Lecturer Bogdan-Cezar CHIOSEAUA, PhD
„Henri Coandă" Air Force Academy
E-mail: b.chioseaua@gmail.com

Rezumat: Apariţia şi evoluţia epidemiei de coronavirus şi transformarea ei ulterioară în pandemie, precum şi modul de răspuns de până acum al autorităţilor, pe etape, la criza generată de către aceasta, ne-a determinat să supunem atenţiei necesitatea stabilirii unor clarificări privind încadrarea ei ca risc sau ameninţare la adresa securităţii naţionale/regionale/globale, utilizând drept fundament teoretic elemente ale gândirii de securitate occidentale şi naţionale.
Cuvinte cheie: pandemie de coronavirus, securitate, ameninţare, risc, vulnerabilitate, strategie de securitate naţională, strategie de securitate internaţională.

Abstract: The emergence and evolution of coronavirus epidemic and its subsequent transformation into a pandemic, as well as the response of authorities – in stages – to the crisis it generated have prompted us to address this issue. Thus, we have felt the need to establish clarifications regarding its definition as a risk or a threat to national/regional/global security, using as theoretical background elements of Western and national security thinking.
Keywords: coronavirus pandemic, security, threat, risk, vulnerability, strategy of national security, strategy of international security.

The coronavirus pandemic is a real challenge to the present time of mankind, but what matters even more are the problematic issues it generates for the future.

Are we going to be able to answer all these challenges?

Among all of them, we chose to attempt an answer to the following question: *Is this pandemic a risk or a threat to national/ regional / global security?*

Even if there is no unanimously accepted definition of security, the one provided by the Copenhagen School researchers[1] managed to organize the Theory of International Relations around this concept[2], as it approached the issue of security from a systemic perspective, using the analysis levels on a space scale, from individual to system through the state and the analysis sector as if being seen through a system of lenses that focus or blur the types of relations and the activity: military, political, economic, social, environmental.

According to theory, national insecurity represents a combination of threats and vulnerabilities – where threats are from outside the system and vulnerabilities are from inside it[3] - and the option of acting upon the causes of vulnerabilities is called national security strategy, while choosing to act in order to reduce or minimize threats is called international security strategy[4].

If we refer to the object of action according to the two options, following the key difference between threats and vulnerabilities, we could say that while vulnerabilities are quite concrete, threats are harder to control because of the subjective-objective ratio between individuals, as well as the difficulty of making the difference between those with an impact upon national security and those resulting from the international competitive environment[5].

---

[1] *N.A.* We are talking about Barry Buzan who, together with Ole Waever and Jaap de Wilde, are representatives of the Copenhagen School that has security as object of study.

[2] *N.A.* Ole Waever about Barry Buzan, according to Barry Buzan, *Popoarele, statele şi frica O agendă pentru studii de securitate internaţională în epoca de după Războiul Rece*, Ediţia a doua, Editura Cartier, Chişinău, 2014, p. III.

[3] *Ibidem*, p. 120.

[4] *Ibidem*, p. 333.

[5] *Ibidem*, pp. 122-123.

At the same time, we need to compare the likelihood of a threat happening with the consequences it might determine[6] with the profound ambiguity of threats[7], as well as the fact they might occur in all sectors (domains or dimensions) mentioned above.

In this regard, it is emphasized that ecological threats, just as the other types of threats, may cause prejudice to the physical background of a state in sufficient measure so as to be able to threaten its idea and institutions[8].

The synchronizing of Romanian security thinking to the Western one, as well as the necessity to broaden the term were materialized in our country by promoting the concept of Extended National Security (E.N.S.) within the Romanian National Defense Strategy (in Romanian Strategia Națională de Apărare a Țării - S.N.Ap.Ț.) for the cycle 2015-2019.

This is based on constitutional democracy and the mutual respect between state and citizens and adds to four of the domains mentioned above – military, economic, social and environmental, the last one being only specified, but not explained – the domains of public order, intelligence, counter-intelligence and security, education, health, energetic, financial, diplomatic, crisis and critical situation management[9].

We notice at this moment in our endeavor that the E.N.S. concept lacks the political dimension and the most important question would be why? – given the fact that the elaboration and application of policies in all domains pertain to politicians, the issue of a state's security is a matter of

---

[6] *N.A.* Ole Waever despre Barry Buzan, conform Barry Buzan, *Popoarele, statele și frica. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Ediția a doua, Editura Cartier, Chișinău, 2014, p. 144.

[7] *N.A.* Ole Waever despre Barry Buzan, conform Barry Buzan, *Popoarele, statele și frica. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Ediția a doua, Editura Cartier, Chișinău, 2014, p. 150.

[8] *Ibidem*, p. 139.

[9] *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume*, Administrația Prezidențială, București, 2015, p. 9.

perception and if perceptions are wrong, they can generate dramatic consequences[10].

As a consequence, we propose that the Romanian National Strategy - S.N.Ap.Ț. – for the planning cycle 2020-2025, which is currently being discussed, should include the political dimension within the E.S.N. while the other dimensions be approached in a succession able to underline its importance within the national security system.

In S.N.Ap.Ț., the definitions of threats and vulnerabilities are based on the key distinction between them, while risk is defined as a possibility of manifestation of an uncertain event with direct or indirect impact upon national security[11].

In addition, in order to create a common conceptual framework, they are approached in the Strategy Guidelines[12].

From the medical point of view, the epidemic represents the rapid development of a contagious disease, within a population, at most times of infectious origin, determined by an endemic or occurring for the first time[13].

The pandemic is an epidemic that expands on a very large territory, comprising several countries, continents[14].

Initially, upon its outburst (which is still debatable with respect to when and where it happened), COVID-19 caused an epidemic which, afterwards, turned into a pandemic.

According to S.N.Ap.Ț., the pandemic is a low probability risk, but with a major impact, the same as the low intensity military confrontations, persistent in time, the migration flows generated by natural catastrophes and ecological disasters[15].

---

[10] *N.A.* The statement belongs to Robert Jervis, according to Radu-Sebastian Ungureanu, *Conceptul de securitate*, in Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), *Manualul de relații internaționale*, Editura Polirom, București, p. 182.

[11] Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019*, *op. cit.*, p. 23.

[12] *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*, Administrația Prezidențială, București, 2015, pp.12, 15, 17.

[13] *[www.csid.ro>Dictionar medical],* accessed on 13.04.2020.

[14] *[dexonline.ro/definitie/pandemie],* accessed on 13.04.2020.

[15] Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019*, *op. cit.,* p. 25.

Yet, a risk generates a crisis most of times and the inadequate management of such a situation – period or tensions, turmoil, trials (often decisive ones) that take place in society[16] - may determine turning the risk into a threat to national security.

In order to prevent the spread of COVID – 19 virus and to perform consequence management, Romanian authorities instituted the state of emergency for a period of 30 days[17] restricting the exercising of certain rights, and establishing two categories of measures: first emergency measures, with immediate applicability (Annex 1 of the Decree) which cover the domains of public order, economy, health, labor and social protection, justice, external affairs etc.; and measures with gradual applicability (Annex 2 of the Decree)[18].

Thus, it can be noticed that, through the measures taken in an interval of approximately 6 weeks from the occurrence of the first case of coronavirus infection, authorities answer a crisis – public health crisis – generated by a risk (the pandemic) acting upon the causes of vulnerabilities of the national system of public health (national security system) to the purpose of limiting its effects.

Through the decision made (the political dimension), there was an involvement of the mechanisms of national system of crisis response (the other dimensions of E.N.S. concept) and in the dynamics of crisis evolution there was a clear picture of what we have and what we do not have in order to face such a situation.

Subsequently, after a period in which member states focused primarily on what was happening „inside" themselves, the European Union started to collaborate with them in order to give a coordinated response, meant to prevent the further spread of the virus and its effects.

In this respect, there were temporary restrictions upon the unessential travels towards E.U. countries, for 30 days; the movement of

---

[16] *[https:// dexonline.ro>definitie>criza],* accessed on 13.04.2020.
[17]   *N.A.* It came into effect on 16th March 2020, date of issuance in Romanian Official Gazette, Part I.
[18]   *[www.pwc.ro],* accessed on 10.04.2020; On 6th April 2020, Romanian President announced that he was going to extend the State of Emergency with 30 more days, until 16th May 2020 (according to *[https://romania·europalibera. >io…],* accessed on 10.04.2020).

European citizens outside E.U. borders was not recommended; the Council activated the integrated E.U. mechanism for political crisis response (IPCR), the European Commission and Council facilitate the permanent contact and coordination of relevant national ministries; the European Council's president organized a conference with E.U. leaders; the European Center for Disease Control and Prevention (ECDC) issued for the E.U. population rapid risk assessments and epidemiological updates[19].

At the same time, the E.U. stated its commitment to countering disinformation and cooperate with member countries in order to ensure equipment, promote research for cures and vaccines (140 million €), support employment opportunities, enterprises and economy (37 billion €), and the European Bank announced a program of emergency acquisitions amounting to 750 billion €[20].

The reaction was slow, from our point of view, both from N.A.T.O. which, starting with 02.04.2020, through its Secretary General, appointed the Supreme Allied Command Europe (SACEUR) to coordinate the necessary support in order to deal with the virus by providing: healthcare professionals; hospital beds and essential medication; medical personnel, essential materials and equipment from civilian and military sources; medical scientific, and technological knowledge and resources[21].

Following the succession of events presented above, in addition to the crisis response to the crisis generated by the pandemic in the first stage – from the identification of the first Romanian citizen infected with COVID-19 up to the initiation of the crisis response mechanisms from the E.U. and N.A.T.O. – in the second phase, together with N.A.T.O. and E.U. intervention, there were, in our opinion, important actions taken in order to reduce and diminish the threat (to the international security crisis).

As a result, the pandemic evolution following the „trajectory" risk-crisis-threat determined the Romanian authorities to act as a first step upon the causes of vulnerabilities (the strategy of national security).

---

[19] *[https://www.consilium.europa.eu>c...],* accessed on 09.04.2020.
[20] *[https://www.consilium.europa.eu>c...],* accessed on 09.04.2020.
[21] *N.A.* Declaration adpted by the Ministries of External Affairs of N.A.T.O. member countries after the reunion on 02.04.2020, according to *[https://www.euroactiv.ro>extern>n...],* accessed on 09.04.2020.

That is the reason why we consider that in the first phase the pandemic was a risk to national security which, in the second phase, turned into a threat.

Thus, the inadequate management of a risk generated its transformation into a threat to national security, having unexpected and unpredictable effects upon the domains of security.

And this is not everything. As the threat was „fulfilled”, states, regions, continents, mankind has entered a period of true „war” against an „enemy” that can „attack” you at any place and time, invisible, without taste or smell, which you sometimes feel, at other times you do not, which does not take into account the geographic location, the geography of the territory, the level of economic development, the type of relation (friend, foe, neutral), the security policies of the „target-states”, which managed to „defeat” state after state, region after region, continent after continent, without facing a sufficiently powerful reaction so as to be stopped on a certain „phase line”.

This is a „conflict” between the human being and the environment, in which the human being did not have enough information about the capabilities, strategies, and intentions of the „enemy” in order to come up with the appropriate reaction and until now there has not been any „commander” yet, who, with the resources available, could use the adequate concepts of conducting „military actions” (the commander's art) so as to accomplish the goal set (the defeat of the „enemy”).

The characteristics of the „aggression” (propagation speed, virus mutations – from one country to another, from one region to another, from one continent to another – dimension, amplitude, intensity, effects produced) and the reaction of the authorities at all levels (national/regional/global) to it, demonstrate once again the fact that the security of the human being is relative, not absolute, and that it is practically impossible to ensure one's security „by oneself”, the international security system remaining yet the desirable option.

There is „something” that mankind has not confronted in the recent past, with effects extremely difficult to quantify upon all the domains of national, regional, and global security.

At the same time with the „fight" of world states against COVID-19 virus, there are „signs" that another one has started, namely, the fight for identifying the „culprit" for everything that is going on nowadays.

Thus, the U.S. President talks about the „Chinese virus", the Chinese officials pretend that it was brought to China by the Americans on the occasion of conducting in Wuhan the Military World Games, during the period between October 18th and 27th, 2019, another report showing that it was the European tourists, not the Asian ones that brought the virus to New York[22].

Furthermore, there is information according to which the Wuhan Virusology Institute conducted experiments on mammals captured at a distance of 1,600 km., in Yunnan region, experiments that were sponsored with 3.7 mil. $ by the American government, and the laboratory is actually the original source of the virus, and not the animal market in Wuhan[23].

In the same vein, a high American official, asked on Wednesday 08.04.2020 if China withheld information upon the spread of the virus, stated that that was not the time for force reactions, but that there is still time for clarity and transparency[24].

Last but not least, the U.S. President cut off financing for World Health Organization (W.H.O.), which, in his opinion, is to blame for the spread of the virus.

Probably, this fight is going to continue even if mankind has to confront and deal with both the coronavirus and the economic crisis that we can all „see" and „feel".

Just as the 20th century managed to solve economic challenges with two main schools of economic thought, that of John Maynard Keyns and that of Milton Friedman which showed – the former – the role of state interventionism in balancing the economic policies of the free market and the unbalances they cause and – the latter – the role of money and financial-banking balances, the 21st century has to face a new type of economic

---

[22] *N.A. This is a report published in New York Times, according to [https://m.digi24.ro>...>SUA], accessed on 12.04.2020.*
[23] *[https://m.mediafax.ro>externe>po..],accessed on 12.04.2020.*
[24] *N.A. State Secretary Mike Pompeo, according to [https://caleaeuropeana.ro>covid-19-secretarul-de-stat-al-SUA-mike-po...], accessed on 13.04.2020.*

crisis, with new challenges never encountered before. This means that it will have to take over the favorable elements in the existing economic theories.

The great economic challenge is finding a new macro-economic policy, a „New Deal" of our times which, just like American President Franklin Delano Roosevelt, we might have the strength to implement, to understand that it is not going to be perfect from the beginning, but rather perfectible all throughout, and yet able to help us find the points of equilibrium between work and profit, the free market and the state-imposed regulations, the need for financing and capitals.

If we paraphrase Friedman's theory regarding „reasonable expectations", maybe this is exactly what the 21st century is expecting from us: to have „reasonable expectations" from ourselves and from state authorities, in all the domains of economic-social life.

As our scientific endeavor has started from the need for clarifications regarding the characterization of the coronavirus pandemic as a risk or as a threat to national, regional, and global security, we consider that it will be the duty of political and military authorities at national, N.A.T.O. and E.U. levels to perform a thorough analysis and make the adequate decision which might modify or not the place of the pandemic in the fundamental documents regarding security.

References

1. Barry, Buzan   *Popoarele, statele și frica – O agendă pentru studii de securitate în epoca de după războiul rece*, Ediția a doua, Editura Cartier, Ediția a doua, Chișinău.

2. Andrei, Miroiu; Radu-Sebastian, Ungureanu (coord.)   Manualul de relații internaționale, Editura Polirom, București, 2006.

3. ***   Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume, Administrația Prezidențială, București, 2015.

4. *** Ghidul Strategiei Naţionale de Apărare a Ţării pentru perioada 2015-2019, Administraţia Prezidenţială, Bucureşti, 2015.

5. *** www.csid.ro>Dictionar medical
6. *** https://dexonline.ro
7. *** www.pwc.ro
8. *** https://www.consilium.europa.eu>c…
9. *** https://www.euroactiv.ro>extern>po...
10. *** https://m.digi24.ro>...>SUA
11. *** ttps://m.mediafax.ro>externe>po...
12. *** https://www.caleaeuropeana.ro>covid-19-secretarul-de-stat-al SUA-mike-po…

DESPRE SECURITATEA NAȚIONALĂ
ÎN NOUL CONTEXT MONDIAL

ON NATIONAL SECURITY IN THE CURRENT WORLD

Ion-Sorin MOLDOVAN, PhD candidate
E-mail:moldovan.ion.sorin@gmail.com
.

Rezumat*: Trăind într-o epocă marcată de o dinamică deosebită, ne confruntăm cu o lume a insecurității, în care se remarcă înainte de toate prăbușirea sau alterarea sistemelor de valori tradiționale, care una după alta devin tot mai desprinse de realitate și mai greu de aplicat; este o lume conflictuală în care formele de confruntare devin însă tot mai atipice, arsenalul mijloacelor de luptă îmbracă forme tot mai puțin convenționale. În acest context foarte complicat, se constată o stringentă, imperioasă nevoie de securitate, indiferent dacă această tendință se exprimă din partea actorilor statali sau a indivizilor; totodată, remarcăm în momentul de față o continuă tendință a lumii de a stabili o nouă stare de echilibru. Aceasta într-o situație fără precedent, pe fondul procesului tot mai intens de globalizare dar și al unei dezvoltări tehnologice fără precedent. Se poate afirma că toate procesele și fenomenele clasice legate de securitate vor căpăta în noul context noi forme și caracteristici, astfel încât vom putea vorbi despre formarea unui climat de securitate cu totul și cu totul nou, care impune modificarea paradigmelor în scopul de a identifica soluțiile eficace.*

Cuvinte cheie: *securitate, seuritate națională, apărare națională, informații, ordine publică.*

Abstract: *Living in an age marked by special dynamics, we are facing a world of insecurity, in which we notice first and foremost the collapse or alteration of traditional value systems, which one after the other are becoming more detached from reality and harder to apply; it is a conflictual world in which the forms of confrontation are becoming increasingly atypical, the arsenal of the means of combat taking less conventional forms. In this very complicated context, there is a pressing, urgent need for security, whether this tendency is expressed by state actors or individuals; at the same time, we are noticing at present a continuous tendency of the world to establish a new state of equilibrium. This is happening in an unprecedented situation, against a background of not only an increasingly intense process of globalization but also of an unprecedented technological development. It can be said that all the classic processes and phenomena related to security will acquire new forms and characteristics in the new context, so that we might be able to talk about forming an absolutely new security climate, which requires changing paradigms in order to identify effective solutions.*

Introduction

Within the specialized literature in the field and given the natural influence of normative acts and other official documents, among which we should underline especially the National Security Strategy elaborated by the Presidency, as a main law source in this domain, there have been frequent attempts at defining the syntagm „national security". We can notice how the strategies prior to year 2015 tried to give clear definitions of the concept. Interestingly enough, the last valid security strategy (issued in June 2015) did not include such a definition, unlike the rest of the strategies, issued prior to this one, which specifically stated that national security is *a state of facts characterizing the nation[1]*, social communities, citizens, and the state.

The same state of facts, in order to reach in itself the state of security, should have as a fundament economic prosperity, legality, a general state of balance (expressed in all the domains of social life and the life of individuals) as well as social and political stability. On the whole, if it exists, the respective state of facts would be concretely expressed through the syntagm „lawful order", whose preservation involves a systemic combination of actions very diverse in nature (political, economic, military, social, juridical, imagological, psychological, information etc.), accomplished by all of them with the final purpose of ensuring the unrestrained exercising of citizens' rights and freedoms. This happens only due to a complete manifestation of the components of state self-determination, through exercising its fundamental attributes deriving from the quality of the state as a subject to international law and actor on the international stage[2].

The events that took place in the last two decades showed us a certain dynamics increasingly difficult to predict and an atypical behavior of internal and international environment, a situation which frequently led to annihilating classical paradigms without being able to simultaneously

---

[1] Romanian Presidency, *Strategia de securitate națională a României*, București, 2007.
[2] Filofteia Repez, Gheorghe Deaconu, Cornel Dinco, *Securitate și insecuritate în era globalizării*, Editura Universității Naționale de Apărare Carol I, București, 2011, pp. 16-21.

replace them with an acceptable updated solution. A possible variant would be returning to the model of the national state and bringing back traditions and traditionalism to the importance it once had, but this solution is fiercely contested by certain circles, especially those pertaining to the financial or commercial fields, which had a lot to gain from the globalization process. Obviously, all these aspects mentioned above will only be able to provide food for thought, at the same time drawing the attention of specialists in military sciences upon the increasingly stringent need of devising new theories, preferably as realistic as possible, regarding the security of nations and the ways of achieving it.

Security, as a permanent need of the individual and collectivity

If we are to begin our analysis regarding the concept of security through a strictly juridical approach, taking into account the concrete ways of achieving it, we notice the following aspects:

• Security undoubtedly is the most important need, thus occupying the superior position in the hierarchy of collective rights;

• There is no true nation (which does not refer only to a number of people brought together because of different causes or by fate) which can resist otherwise than by achieving that state of facts which is circumscribed to the state of security;

• In concrete terms, the state security is based on is materialized as a systemic combination of norms, different types of actions and measures meant to lead to the achievement of that state of facts;

• Last but not least, the state of a nation is always conditioned by the geographic (geopolitical) and historic context, against the backdrop of the dynamics on the international stage, the structure of the actors and the relations that represent and characterize this scene[3];

• Taking into account what was mentioned above, it is obvious that the state of a nation will become first and foremost characterized by the elements specific to national security, as it is impossible to conceive it otherwise than as a unitary and undividable system; the analysis of the

---

[3] Filofteia Repez, Gheorghe Deaconu, Cornel Dinco, *Securitate şi insecuritate în era globalizării*, Editura Universității Naționale de Apărare Carol I, București, 2011, pp. 34-51.

elements belonging to this system offers us an image upon the configuration and stability of a nation, or at least the basic indicators of the stability of a society and the strength of the state built around a nation.

According to these characteristics, as they were presented above, we could state that national security could be characterized through a series of essential aspects such as:

➢ It permanently stands for that *unifying* or *integrative* framework for all its components, whose wellbeing results in security, which it maintains inter-connected in a coherent structure and normally it also strengthens;

➢ Generally speaking, security is the most accurate reflection of the *constitutional order* and, thus, it becomes the foundation or the resistance structure for accomplishing and maintaining the nation and the nation-state;

➢ Within the law system, security is an integrating concept *as well as a goal*, a central benchmark, occurring as *an inalienable and never-ending law*, universally opposable to any actor on the international stage, to any internal force, and which should normally be based on the traditional value systems;

➢ Practically, security cannot be achieved otherwise than in the context given by regional and global security, actually depending on it.

According to these observations, it becomes really clear that there is a crucial need for achieving (and maintaining) the state of security (real security, not only the perceived one), through a continuous adaptation or intervention (when it is necessary) upon the dynamics of the geopolitical environment and in the matter of interactions with other actors of the international environment.

Components of security and national security

Structurally, security is a system made up of five apparently autonomous components: *economic*, *political*, *military*, *social* and *environmental security*. Particularly speaking, however, *national security* cannot be described through the simple analysis of its components, but through their practical means of achievement. Our analysis gives importance to this aspect, especially due to the fact that lately the correct

meaning of the terms „*security*" and respectively „*defense*" have seemed to be characterized by confusion.

As if coming to increase these undesirable mistakes regarding the right meaning, in the summer of 2015, Romanian Presidency elaborated the official document entitled „Romanian National *Defense* Strategy", instead of using the name „security strategy", thus implying that the President may have focused only on certain components of military security, thus wishing that these official documents referred in a strict and limiting manner only to *defense*, and not to the other components of security.

Passing over such official approaches that we have considered at least confusing, in not entirely erroneous, we may state that (national) security is composed of a series of composing elements as follows:

➢ **National defense**, about which (starting from the definition included in the law[4]) it is said that it represents a systemic group of *actions and measures taken by specialized authorities of the state, in order to defend and guarantee national sovereignty, independence, and state unity, territorial integrity, and constitutional democracy*; the analysis of this text shows clearly that national defense refers only to a well-identified and delimited component of security, thus on no account being able to include security on the whole, but constituting only the essence of the military component of security.

In connection to national defense, we cannot help but notice how lately (in the last couple of years) its content has tended to become increasingly ambiguous, a state of facts created by the general tendency (caused by globalization as well as by other processes of contemporary phenomena[5]) of diminishing the aspects related to the principle of self-determination, among which the most important ones are, undoubtedly, independence and sovereignty. The present moment shows us a certain trend of considering these two values somehow obsolete, even if they have always represented, since ancient history, supreme vales. Following the model of the old empires (Roman Empire, British Empire, Austro-Hungarian Empire

---

[4] According to Law no. 45/01.07.1994 *Legea apărării naţionale a României*, publicată în M.Of. nr. 172/07.07. 1994.

[5] C. Moştoflei, P. Duţu, *Apărarea colectivă şi apărarea naţională*, Editura Universităţii Naţionale de Apărare, 2004.

etc.) in the new international organizations (as is the case of the EU) the tendency is that member states find limitations exactly in those attributes of self-determination. Such situations are not new at all, being encountered especially if we are studying the administrative division of the great empires of the last centuries. In those cases, either one or several of the states had indeed the role of leader and enjoyed the attributes of self-determination, while the other nations which functioned as if under occupation, implicitly, only had the right to exist as more or less autonomous regions. Nowadays, within the EU, there still are states that have preserved intact all their attributes to self-determination, while smaller states (for instance, those in the East of Europe) were one way or another compelled almost to give up entirely exactly the supreme values pertaining to the national state: *independence and sovereignty*.

➢ **National safety** represents another basic component of security, comprising a number of norms, actions, and measures established by law[6] which are concretely destined to the state guaranteeing not only constitutional order, but also fundamental values that are stipulated by the Constitution, generally speaking the so called democratic values, the rule of law and, last but not least, the safety of all citizens.

It is considered that safety is ensured, practically, through all the (counter)intelligence and security actions (here security being used in the sense of providing guarding and protection) regarding certain people and/or objectives. Similarly, national safety may just as well refer to the guarantees made by the state to the address of the nation, from the perspective of achieving, as well as preserving, its needs and interests of security. We also need to mention here the fact that safety also refers to fulfilling that specific function of security, namely the *prediction function,* producing effects with respect to preventing surprises of any kind which might harm or cause any kind of detriment to security.

According to the law quoted above, the concept of national safety refers to the *state of legality, balance, and social, economic, and political stability necessary for the existence and development of the national Romanian state as a sovereign, unitary, independent, undividable state, the*

---

[6] *Law no. 51/1991 privind siguranța națională a României*, publicată în Monitorul Oficial nr. 163/07.08.1991, republicată în Monitorul Oficial nr. 190 din 18 martie 2014.

preservation of the rule of law as well as the climate of unrestrained exercising of fundamental rights, freedoms, and duties of the citizens, according to the democratic principles and norms established by Constitution. The very text of this definition given by the law leads us to the idea that safety state cannot be other than directly connected to the state of legality, yet also conditioned by the existence of a balance at social level. Furthermore, the law states that national safety is *achieved through acknowledging, preventing, and removing internal or external threats.* From this provision of the law we can only notice *the common aspects* dealt with by national defense and safety.

<div align="center">*</div>

Nevertheless, coming back to the previous statements, we consider that official acts (especially those that have normative power) should identify in a more exact manner the meaning of the notions of *defense* and *security*, in the sense that they should be able to establish in a much more precise manner the domain of applicability and thus to establish in a much clearer manner the content of the specific activities and the domain of applicability in each of the two cases. As long as this confusion between security and defense is perpetuated, it will be impossible to accomplish them exactly because of maintaining this confusion upon two domains that have obvious differences in content.

➢ **Public Order** represents, according to the provisions of the law[7], *a spectrum of political, economic, and social norms and measures* which should allow a generally normal functioning of state institutions and, not the least important, which should ensure maintaining public calm and normality together with guaranteeing citizens' daily safety, as well as the continuous observation / protection of individuals and communities' rights.

Taking into account the presence of the five components of security (political, economic, military, social, environmental) as well as this special dynamics of the modern world, at the backdrop of an extremely rapid technological evolution, we can notice that both the generic concept of security and, especially, that of national security have acquired other and other meanings and composing elements. An important aspect in reconsidering the concept of security was the multidimensional character of

---

[7] According to *Strategia națională de ordine și siguranță publică 2015-2020*, Ministerul Afacerilor Interne, București, 2015.

modern confrontation[8], a situation which brought more and newer elements in the equation of security, most of the time complicating a lot this equation.

All these aspects mentioned above have led to the current situation in which security seems to be an increasingly complex domain which exceeds any predictive attempt.

Conclusions

Following our brief analysis and taking into consideration the critical aspects mentioned, we can conclude that:

➢ there is still no centralizing normative act regarding security; this has to be simultaneously included in an official document with the power of a normative act, under all its aspects and regarding all its components;

➢ the system of security, as it is conceived at present, is unable to respond to unconventional actions (with or without NBC means) in asymmetric, hybrid format;

➢ nowadays, population has been completely eliminated from the actions and measures regarding security, as there is no active involvement from its part in activities meant for security.

Such aspects create the premises of a significant dysfunctionality within the security system and raise fears regarding the capability of this system to react rapidly and in an efficient manner in serious cases.

References

1.   ***   *Strategia de securitate națională a* României, Președenția României, București, 2007

2.   ***   *Strategia națională de apărare a țării pentru perioada 2015-2020,* Președenția României, București, 2015.

3.   ***   *Strategia Națională de Ordine și Siguranță Publică 2015-2020*, Ministerul Afacerilor Interne, București, 2015.

4.   ***   *Concepția de înzestrare cu sisteme și echipamente majore a Armatei României în perioada 2006-2025*, Ministerul Apărării Naționale, București 2006.

5.   ***   Ordonanța de urgență a Guvernului nr. 1 din 21.01.1999

---

[8] Lucian Stăncilă, *Acțiuni militare în câmpul de luptă modern*, Editura UNAP, București, 2004.

6.	***	publicată în M.Of. nr. 22 din 21.01.1999 privind Regimul stării de asediu și al stării de urgență.
7.	Moștoflei C.; Duțu P.	Ordonanța de urgență a Guvernului nr. 21 din 2004 privind *Sistemul Național de Management al Situațiilor de Urgență* *Apărarea colectivă și apărarea națională*, Editura Universității Naționale de Apărare, 2004.
8.	Repez, Filofteia; Deaconu, Gheorghe; Dinco, Cornel	*Securitate și insecuritate în era globalizării*, Editura Universității Naționale de Apărare Carol I, București, 2011.
9.	Stăncilă, Lucian	*Acțiuni militare în câmpul de luptă modern*, Editura UNAP, București, 2004.

DE LA ATRIBUȚIE LA MISIUNE. OPERAȚIONALIZAREA ATRIBUȚIILOR JANDARMERIEI (I)

FROM JOB DESCRIPTION TO MISSION. OPERATIONALIZING THE TASKS OF THE GENDARMERIE (I)

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

Rezumat: *Articolul de față aduce în dezbatere relația dintre atribuție și misiune așa după cum sunt ele precizate în legea de organizare și funcționare a Jandarmeriei Române, deși nu se fac distincții clare între acestea și nu este dezvoltată o viziune asupra modului de operaționalizare a atribuției în raport cu circumstanțele situației în care sunt angajate structurile specializate de jandarmi. Totodată, specializarea impune o delimitare clară și asupra domeniului de acțiune, o definire a standardelor de acțiune, a principiilor și tacticilor speciale. În același timp, o astfel de relație vizează și procesul de planificare, organizare, conducere și executare a unei acțiuni cu finalitate propriu-zisă în misiune (scop, obiectiv), modul cum este proiectat acest întreg proces dinamic și cum se încadrează misiunea în atribuție.*

Cuvinte cheie: *atribuție, misiune, formă de acțiune, procedură, forțe.*

Abstract: *The present article brings into discussion the relationship between the task and the mission as spelled out in the law on the organization and functioning of the Romanian gendarmerie, although there are clear distinctions between them and there is no vision on the organization of the task in relation to the circumstances of the cases in which the specialized structures of the police are employed. At the same time, specialization imposes a clear delimitation on the scope of action, and definition of action standards, principles and special tactics. Moreover, such a perspective also concerns the process of planning, organization, management and execution of an action with proper purpose in the mission (purpose, objective), how this whole dynamic process is designed and how the mission fits the legal vocation.*

Keywords: *assignment, mission, form of action, procedure, mission, forces.*

The present article debates aspects related to the operationalization of duties in relation to the situation of gendarme troops' engagement and, implicitly, their nature. From both theoretical and practical

perspective, this relation implies a process of planning, organizing, conducting, and executing an action, in correlation with both the domain of the duty and its purpose. Although stipulated in military regulations, this process needs adapting to the police nature of gendarmerie duties, as the respective relation is established with the citizen, not with an enemy in a conflicting, military sense of the term. At national level there is still no model of public order capable to operate with standardized and authorized instruments regarding the culture of law enforcement in the public order domain. It is even imperative that such a culture develop in this domain as this might lead to planning, organizing, and conducting actions in a vision that is much more flexible, balanced, and even instinctive.

As provisioned in article 4 of the law[1], there are, among others, two fundamental characteristics of gendarmerie, namely that of „specialized institution of the state, with military statute", and „organization according to military principles, as a unitary system of forces and means". The main issue for debate is focused on the idea of accepting, acknowledging, legitimizing gendarmerie as police force, because according to these two characteristics, there is a tendency to consider gendarmerie as an intermediate force between the army and the police, based on a „warrior" culture, whose approach is authoritarian, which may affect the legitimacy

---

[1] Art. 4, line. (1) – Romanian Gendarmerie is organized on military principles, as a unitary system of forces and means, arranged according to the administrative-territorial organization of the country, and has the following organizational structure:
a) General Inspectorate of Romanian Gendarmerie, to be called in the following lines General Inspectorate;
b) General Gendarme Directorate of Bucharest;
c) Special Brigade of Gendarme Intervention and mobile gendarme task groups;
d) county gendarme inspectorates;
e) military education institutions for the training and life-long learning of personnel;
f) specialized units and sub-units, necessary for accomplishing the duties specific to Romanian Gendarmerie, including of logistic and medical support, established according to the law.
(2) Upon the proposition of the general inspector of Romanian Gendarmerie, the Minister of Administration and Interior, according to the dynamics of gendarmerie duties and missions, may found, dismantle, deploy and re-deploy units, up to brigade echelon exclusively, under the provisions of the law, services, sections, offices, compartments, and gendarme sub-units, within the limits of positions approved and budgetary funds allocated.

and trust of the citizens while, actually, the actions executed are rather related to the police actions, having as fundamental aims guaranteeing freedom of expression and ensuring the optimal conditions for a climate of security. The very expression „restoring public order" may determine from the start an attitude of combating protests from the perspective of its specialized function, but without taking into account the crowd behavior as an extremely complex variable or the fact that „emotion is a basic feature of human condition, with consequences"[2] many times even unpredictable. From this perspective, due to the „continuous increase in threats and crimes that society is facing and the limited available resources meant for facing them, police agencies need to develop programs focused on pre-emptive measures and the identification of emergent threats (...) through the pro-active identification of indicators and taking measures based on information"[3].

Taking into account the fact that the organizational structure of the gendarmerie includes Bucharest General Directorate of Gendarmerie, Gendarmerie Special Intervention Brigade, Mobile gendarme task force, County gendarmerie inspectorates and Specialized units, and that each such structure includes a „command structure", including at the level of Specialized gendarme battalion, subordinated to the Special Brigade, we have a clear picture of conceptual support for actions. After thirty years of performing a large diversity of actions, irrespective of their amplitude, density, and intensity, it results that there are sufficient arguments to serve as starting points for doctrine concepts comprised in a manual in the field.

At the same time, the law operates with two terms: (specific) missions and attributes, which necessitate a few conceptual clarifications, as long as in the law, regarding duties, the text enumerates the missions by correlation with the military statute of the gendarmerie, the organization on military principles, the unitary system of forces and means. Also, another syntagm

---

[2] Alexander J. Shackman, Richard J. Davidson, *The Nature of Emotion. Fundamental Questions*, Second Edition, Oxford University Press, 2018, p. 420.
[3] Nate Huber, *Intelligence led policing for law enforcement managers*, in FBI Law Enforcement Bulletin, October 2019, https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers, accessed on 17th January 2020.

used is „the accomplishment of main and support functions"[4] in emergency situations[5].

We consider that it is phrases such as „conduct missions of ensuring public order", „execute missions of restoring public order" that cause confusion at conceptual level, as long as for such actions specific to public gatherings, the actions conducted by gendarme structures are conceived, planned, and organized by deliberation, and at European level and not only there are other approaches regarding crowd control and crowd management. This led to setting up the exact ways of approaching crowd events: force escalation, negotiated management, command, control, and strategic incapacitation, approaches which actually do not exclude each other.

Given the process of planning, organizing, and conducting such actions which are finalized through an operational plan, there results the need to identify and define the tactical action (operation) in all the

---

[4] http://www.jandarmeriaromana.ro, accessed on 12th December 2019.

[5] It ensures measures for maintaining, ensuring, and restoring public order; it ensures the judicial planning of resources available in order to accomplish specific missions; it participates in planning and ensuring the operational capabilities necessary for clearing access ways in the area affected by an emergency situation, in order to save human lives and facilitate the access of emergency structures to the affected locations; it participates in search and rescue actions; it ensures measures of protection of areas where there is an imminent danger of emergency situations and of population evacuation; it ensures securing and monitoring the areas affected/evacuated and other resources, as well as distributing water and food for the people or animals affected or evacuated; it applies measures of ensuring public order and protection of areas in which there has occurred or there is an imminent danger of occurrence of some emergency situations and re-establishing public order in the affected area and in its immediate vicinity; it participates in ensuring the protection of transports with humanitarian aids and distributing them; it ensures security during the evacuation of population and material goods; it provides guard and security of the perimeter of areas of intervention/quarantine; it provides guard and security of evacuated areas; it supports the evacuation of people, animals and goods and setting the camps/places destined to people evacuated; it participates, in support of inspectorates for emergency situations, with forces and means, in ensuring reaction and removing the effects produced by the emergency situation; it ensures reconnaissance, research, field assessment and primary reporting of the emergency situations consequences; it ensures monitoring the specific risks and hazards; it participates in establishing and preparing the boarding points for the people evacuated from the affected areas; it ensures communication and IT connections for own structures - http://www.jandarmeria romana.ro, accessed on 12th December 2019.

complexity of its content and physiognomy. This is actually a management option and, as an operative document, we propose an „Operational plan for the management of public gatherings (crowd event)". Regarding the provision according to which it „executes missions for restoring public order", the approach is quite simplistic. It is increasingly difficult in the current context to conceive from the start the restoring of public order when protests are increasingly professionalized, the participants being fully aware of the legislation in the domain of public gatherings, the rights they have, the obligations and limitations of law-enforcement. It is obvious that protests have evolved, there are new tactics of intimidating law-enforcement troops, of provoking them to use force, of drawing the attention of the media.

Our option is in favor of crowd management and control, supporting freedom of expression and protecting the safety of participants, facilitating protest and differentiating among the punctual interventions of law enforcement as, actually, „law enforcement should be the last measure resorted to, following a wide range of preventive efforts"[6]. In such situations we also have in mind the fact that „public order and public freedoms are two concepts better understood together than separately. If we look at each of them, it is not easy to define their framework,"[7], especially as „public order is a fundamental and a little poly-sematic concept"[8].

Command structures are organized in services, compartments, battalions, detachments /companies, sections, platoons, stations, groups, logistic support, medical support or other support structures. The command structure has the responsibility to plan, organize, lead, and coordinate the specific actions executed by a gendarme structure. We consider that the whole process of planning, organization, leading, coordinating, and

---

[6] *Public sector achievement in 36 countries. A comparative assessment of inputs, outputs and outcomes*, The Netherlands Institute for Social Research, The Hague, December 2015, p. 133.
[7] Bernard Stirn (Président de section au Conseil d'État), *Ordre public et libertés publiques*, Intervention du 17 septembre 2015 lors du colloque sur l'Ordre public, organisé par l'Association française de philosophie du droit les 17 et 18 septembre 2015, https://www.conseil-etat.fr/actualites/discours-et-interventions/ordre-public-et-libertes-publiques, accessed on 29th January 2020.
[8] *Ibidem.*

executing actions needs to be rethought as being specific to a police force with military statute, for applying the law in the public order sector. Even if there are duties specified for the state of siege, upon mobilization, and at war, in its quality of part of the armed forces too, there is a need for operative dimensioning and projecting the combative capacity and capability for such situations, underlining the fact that such actions are limited in time and space. Thus, there is a need for differentiating between the initial training and life-long learning of the personnel, in relation with doctrine concepts in the field, the adequate endowment, etc. especially since it is quite difficult to define legal concepts without being able to verify their applicability in the field.

The unitary system of forces require „creating a common understanding of the operational environment, the actions' goals, the problems and their approaches for solving, as a challenge for commanders and personnel"[9]. If we analyze equally the missions and the duties, as they are specified in the law, although there is no clear delimitation as far as they are concerned and there is no explicit provision regarding the police force statute of the gendarmerie, we still consider that engaging gendarme structures in the field of public order show the police nature of actions that presuppose operational strategies specific to any police force which does not have a military statute, although we notice a tendency of militarization as far as it is concerned, regarding endowment. Maybe that is exactly the reason why this unitary system of forces imposes a modern approach of applying the law in the field of public order in relation to specific evolutions.

Practice shows that the most frequent actions performed by gendarme structures pertain to the field of public order, fact which leads to the idea that gendarmerie is a police force, dealing with public order. Actually er also notice the military character of a police force – gendarmerie – through organization, statute, culture, traditions. In fact, from this perspective, „the academic debate regarding the militarization of police is also concentrated on the development of democracies that raise questions regarding the

---

[9] Nathan K. Finney, Jonathan P. Klug, *Mission Command in the 21st century: Empowering to Win in a Complex World*, Fort Leavenworth, Kansas, The Army Press, 2016, p. iii.

democratization / demilitarization of police forces in order to answer all the demands of a modern constitutional state"[10].

In the table below we can see a differentiation among missions and duties, although within duties we also find some missions which are considered as duties. Thus, there is a need for a conceptual understanding of mission and duty. According to the dictionary, by mission we understand „tasking somebody with doing a certain thing"[11], „the task that somebody receives or assumes"[12] or „role, purpose, destination"[13]. Thus, we can also talk about other meanings of the mission: diplomatic mission, school mission, church mission, permanent mission (UN), space mission, peace keeping missions etc.

From a military perspective, by mission we understand „the task together with the aim which indicate clearly both the action that needs to be taken and the reason for it"[14] and, when referring to lower tactical echelons, „the assignment given to a person or a unit; an undertaking"[15]. Duty represents „the field of authority, competence, activity of a person; assignment given to somebody to accomplish"[16]. It may be inferred that all these tasks and duties have a certain specific character determined by the military statute of the gendarmerie, police-like by nature, in case of some of these tasks, for respecting human rights, respecting certain standards of law-enforcement, the urgency of their fulfillment, abiding by certain principles in the use of force, in the use of protection and intervention in law enforcement, etc. If we refer to the content of art. 1 and 2 of the law[17], we

---

[10] Marleen Easton, *Military Policing*, The Sage Encyclopedia of War: Social Science Perspectives, Sage Publications; 2017, p. 1117.

[11] *Dicționar enciclopedic*, Editura Cartier, ediția a V-a, revizuită și actualizată, 2004, p. 541.

[12] *Ibidem*.

[13] *Ibidem*.

[14] Department of Defense, *Dictionary of Military and Associated Terms*, p. 144, https:/ /www. jcs.mil › Portals › Documents › Doctrine › pubs › dictionary.

[15] *Ibidem*.

[16] *Dicționar enciclopedic*, Editura Cartier, Ediția a V-a, revizuită și actualizată, 2004, p. 71.

[17] Art. 1. (1) Romanian Gendarmerie is the specialized institution of the Romanian state, with military statute, component of the Ministry of Administration and Interior, which exercises, within the provisions of the law, the duties it has with respect to defending public order, citizens' fundamental freedoms and rights, public and private property, preventing and disclosing crimes and other misdemeanors or breaking current laws as well as the

can define the domain of authority, of competence, as being public order perceived as a certain regime of society and maintaining it pre-determined security and public stability"[18].

Missions	Manner of execution	Duties	Manner of execution
a) In conditions of normality (at peacetime), as a specialized institution, with a military statute, as a police force, part of the Ministry of Internal Affairs			
Actions, missions of peace keeping, art. 3, aln. (2)	Participation, accomplishment, art. 3, line (2)		
Specific missions in Bucharest – DJMB, art. 8, line (1)	Planning, organization, leading, execution	**Duties** in Bucharest, DGJMB, art. 8, line (1)	Accomplishment
Missions of ensuring and restoring public order, ensuring the protection of state fundamental institutions and neutralizing serious threats regarding them, Bg.S.I.J.R., art. 9, line (1)	Execution – independently or in cooperation, ensuring, neutralization, Bg.S.I.J.R., art. 9, line (1)		
Specific missions, IJJ, art. 10, line (1)	Planning, organization, leading, execution, IJJ, art. 10, line (1)	**Duties**, IJJ, art. 10, al. (1)	Accomplishment
Missions of ensuring and restoring public order	Organization, execution, G. Mb. J.,	**Duties**, specialized	Defense, **mission** execution, **missions** upon request,

protection of fundamental institutions of the state and combating terrorist acts. (2) Romanian Gendarmerie, through duties, organization, preparation, and territorial arrangement, contributes to guaranteeing sovereignty, independence, authority, unity and state security, constitutional democracy on the entire national territory both at peacetime and in crisis situations.

Art. 2. Romanian Gendarmerie conducts its activity in the interest of citizens and community and in support of state institutions, exclusively on the basis and for the abiding of the law.

[18] Vladas Tumalavičius, Jānis Ivančiks, Oleksandr Karpishchenko, *Issues of Society Security: Public Safety under Globalisation Conditions in Lithuania*, Journal of Security and Sustainability Issue, 2016 June Volume 5 Number 4, pp. 547 – 548.

Missions	Manner of execution	Duties	Manner of execution
and combating crime, G. Mb. J., art. 11, line (1)	art. 11, line (1)	structures, art. 19, line (1), art. 20, line (1)	**mission** execution based on cooperation plans, execution in cooperation, **mission** execution for anti-terrorist intervention, ensuring guard or protection, participating in **mission** cooperation, participating in cooperation, participating in **missions** outside Romanian state borders, ensuring order and protection measures, making the necessary paperwork for criminal indictment
Specific missions, B.J.S., art. 12, line (1)	Execution, B.J.S., art. 12, line (1)		
Missions of guard or protection and defense of objectives, goods, high-importance assets, other **missions** in a certain domain of competence of the gendarmerie, U.S., art.14, line (1) .	Execution, U.S., art.14, line (1)		
Specific missions, Dt, Cp., Pl., art. 13.	Accomplishment, independently or in subordination to Dt, Cp., Pl., art. 13.		
b) During the state of emergency – as a specialized institution, with military statute, part of the Ministry of Internal Affairs			
Specific missions, state of emergency, art. 21	Accomplishment, application of military decrees, art. 21		
c) During the state of siege, upon mobilization and at wartime – also as part of the armed forces			
		Duties stipulated at art. 19, duties as a component of the armed forces art. 22, line (1).	Accomplishment of the duties stipulated at art. 19 – execution, participation, ensuring, execution in cooperation, execution of any other missions

Table no. 1 Differentiating the missions and duties pertaining to specialized gendarmerie structures

Nowadays, both police and gendarmerie are „the most visible manifestations of the governmental authorities responsible for public security (...) and need to function in accordance with national and international laws and respect human rights at any moment"[19]. The great challenge for almost all the public order forces are the protests that take a large variety of forms of expression due to their character of spontaneity and lack of regulations and which, „under the influence of the internet and social networks are increasingly frequent"[20], are „largely movements without leadership, with little commitment to traditional groups or ideologies"[21]. A lot of protests seem to be „fueled by the new communication technology and show a common reduced vision upon the constitution of institutions beyond a rejection of existing elites and recognized structures of power"[22]. This kind of civic mobilizations impose to the public order forces the adjustment of response tactics appropriate for the forms of manifestation and the aims of protests. We should also keep in mind the fact that „as they are open, boundless networks that are constantly reconfigured according to the level of involvement of the population in general, this decentralized structure opens up new opportunities of joining the movement and also reduces the vulnerability of the movement to repressive threats, as there are few specific targets which might be quelled, except for occupied places"[23]. In connection to these elements of novelty regarding the manifestation of protests in the public space, there is a need for revision and consolidation of law enforcement regarding the issue of civil freedoms during public gatherings, „the uniform application of standards regarding the use of force, elaboration

---

[19] *Guidebook on Democratic Policing by the Senior Police Adviser to the OSCE Secretary General*, Vienna, May 2008, 2nd Edition, p. 6.
[20] *Facilitating Peaceful Protests*, Academy Briefing, No. 5, Geneva Academy of International Humanitarian Law and Human Rights, January 2014, p. 12.
[21] Thomas Carothers and Richard Young, *The Complexities of Global Protest*, Carnegie Endowment for International Peace, 2015, p. 4.
[22] *Ibidem*.
[23] Manuel Castells, *Comunicare și putere*, Editura Comunicare.ro, 2013, p. xxxix.

of clear instructions regarding the need for self-control, teamwork and obeying orders"[24].

Returning to missions and duties, we need to bring forth the notion of forces and means used for the conduct of a public gathering in conditions of safety, by which we understand the „engagement" of personnel in specialized structures, protection means, support equipment, a combination of those, which is finally configured as a form of specific tactical action, tactical gendarme action (tactical police action, police operation). This is also expressed through the manner, position, attitude in which the available forces and resources are synchronized in time and space, depending on the purpose (regarded as end-state, result, aim, mission), strategies and tactics, as options for executing simultaneous, successive and sequential actions, which are built around the democratic values of respecting the fundamental rights of people in a democratic society.

In connection to the structures of the armed forces, the type of action also underlines the attitude adopted as a response to the enemy's attitude; in other words, there is a need for action coming from an enemy that endangers territorial integrity, independence, and state sovereignty. We have to specify, though, that for gendarme forces with duties in the field of public order, the response expressed as an attitude is towards the event involving the crowd, ins manifestation in relation to the law and, more importantly, the requirement of protecting and guaranteeing constitutional rights. We consider that in this case we are rather in the situation of crowd management, crowd control, as a police operation and not in the situation of adpting a form of action. The common core consists in planning, organizing, and conducting activities and measures on the basis of an operational plan through which to ensure the safety of participants in a gathering and, implicitly, of protection forces, protection of assets, etc. The central issue here is maintaining a balance within the relation authority – freedom, so as through the means and methods specified by law to protect „life, corporal

---

[24] Tony Narr, Jessica Toliver, Jerry Murphy, Malcolm McFarland, Joshua Ederheimer, *Police Management of Mass Demonstrations: Identifying Issues and Successful Approaches*, Police Executive Research Forum, 2006, p. 22.

integrity and freedom of the person, public and private property, legitimate interests of citizens, community, and state"[25].

In the situations in which several specific tactical actions are conducted, the gendarme tactical operation is configured. The respective action is essentially a sum of measures and activities conceived, planned, organized and conducted for accomplishing a mission, for achieving a certain specific aim. For the specific actions in the field of public order, in the planning process „planners need to establish the mission of protecting the constitutional rights of all participants, offering at the same time, a safe and peaceful environment. It is essential that this vision be shared to the whole planning team, strengthened by training and monitoring during the event"[26]. The inexistence of manifestation of an enemy from the perspective of military conflicts, in the public order domain, especially during the events involving crowds, results in our impossibility to consider adopting and operationalizing a type of action, but rather crowd management focused on ensuring the protection and safety of participants.

Certainly, here we can also talk about the need of an action plan (operational plan) designed and conceived on three phases, the pre-event phase, the operational phase (during the event) and the post-event phase, in which tactical communication is essential. The whole planning process has as a result the action plan (operational plan) on the basis of which the tactical action or the political action is conducted.

For the public order domain we need to also keep in mind that „law enforcement answers to a large range of incidents and security operations that are usually managed by a single unit or department"[27], hence the need to create a system of incident management, specifying that the attributes of coordination and leadership are assigned to that force that has competence over the domain, has most of the forces, and has operationalized leadership positions. Taking into account all the information presented and with a view to updating the law of organization and functioning of gendarmerie through

---

[25]Art. 19, alin (1), lit. a), Legea nr. 550 din 29 noiembrie 2004 privind organizarea şi funcţionarea Jandarmeriei Române, *Monitorul Oficial al României* nr. 1175 din 13 decembrie 2004, cu modificările ulterioare.

[26] Bureau of Justice Assistance, *Managing Large-Scale Security Events: A Planning Primer for Local Law Enforcement Agencies*, May 2013, p. 18.

[27] *Ibidem*, p. 33.

which missions are clearly delimited from duties and, implicitly, to elaborating a manual of gendarmerie actions, as a methodology of applying the law through which the typology of actions might be defined, we propose for debate the response as a type of action, excluding reaction, with the necessary peculiarities and adjustments, in civil emergency situations, other than those related to crowd events.

All these have a substantial effect and bring a contribution to redefining, adjusting, and modernizing the specialized tactics (for gendarmes) which essentially refers to „capacities, techniques, and procedures which can be measured, quantified, and used for accomplishing specific tasks"[28]. It has already been acknowledged that „tactics also necessitates adjustment to the unique circumstances of a situation in which the techniques and procedures adopted, as models or established processes, may also lead to the creation of new techniques and procedures"[29] as standard, detailed steps that need to be taken for accomplishing the specific tasks.

In the specialized literature in the field, there is also another phrase – action procedure (fight) which may be defined as a modality of action, being more limited in time and space than the action type. It is obvious that the action type is expressed through tactics, action procedures, techniques and procedures that have mission accomplishment as an end-state and which it influences in turn, making the type of action experience a process of inter-relating these elements and, at the same time, modernization. Techniques are detailed methods, used by forces of commanders in accomplishing the tasks assigned. They describe „the main elements in using equipment and personnel"[30]. Procedures are concretized in „the lowest level of details of a certain course or manner of action, describing the way of performing a certain task"[31]. All these procedures, techniques and processes, through their permanent character, include „manners of operating for weapons and

---

[28] *ADP 3-90 Offense and Defense*, Headquarters Department of the Army Washington, DC, 31 July 2019, pp. 1-3.
[29] *Ibidem*, p. 1-1.
[30] *Field Manual, FM 3-19.1 Military Police Operations*, Headquarters Department of the Army, Washington, DC, 22 March 2001, Appendix B Doctrine and Training Literature, 22 March 2001, p. 2 of 2.
[31] *Ibidem.*

equipment, actions of the forces and their coordination"[32] and have as an end-state the „unitary character of an action, its efficiency, and the mutual completion of layout elements"[33].

References

A. Official documents

1.   ***   *Constituția României*, Monitorul Oficial al României, Partea I, nr. 233 din 21 noiembrie 1991, modificată si completată prin Legea de revizuire a Constituției României nr. 429/2003, Monitorul Oficial al României, Partea I, nr. 758 din 29 octombrie 2003.

2.   ***   *Legea nr. 550 din 29 noiembrie 2004 privind organizarea și funcționarea Jandarmeriei Române*, Monitorul Oficial al României nr. 1175 din 13 decembrie 2004, cu modificările ulterioare.

3.   ***   *Legea nr. 60 din 1991 privind organizarea și desfășurarea adunărilor publice*, Monitorul Oficial al României, Partea I, nr. 192 din 25 septembrie 1991, republicată.

4.   ***   *Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad*, Boletin Oficial del Estado núm. 63, de 14 de marzo de 1986, España.

5.   ***   *Guidebook on Democratic Policing* by the Senior Police Adviser to the OSCE Secretary General, Vienna, May 2008, 2nd Edition.

6.   ***   *The Anthology GODIAC – Good practice for dialogue and communication as strategic principles for policing political manifestations in Europe*, Polisen, With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission – Directorate – General Home Affairs and the Swedish National Police Board, HOME/2009/ISEC/AG/182, 2013.

7.   ***   *Instruction du 21 avril 2017 relative au maintien de l'ordre public par la police nationale*, Bulletin Officiel du Ministere de l'Interieur.

8.   ***   *ADP 3-90 Offense and Defense*, Headquarters Department of the Army Washington, DC, 31 July 2019.

9.   ***   *Crowd Dynamics in Public Order Ops*, UN Peacekeeping PDT Standards for Formed Police Units, 1st edition, 2015.

10. ***   *Field Manual, FM 3-19.1 Military Police Operations*, Headquarters Department of the Army, Washington, DC, 22 March 2001, Appendix B Doctrine and Training Literature, 22 March 2001.

---

[32] *Ibidem.*

[33] *Ibidem.*

11. *** *Facilitating Peaceful Protests*, Academy Briefing, No. 5, Geneva Academy of International Humanitarian Law and Human Rights, January 2014.

12. *** Bureau of Justice Assistance, *Managing Large-Scale Security Events: A Planning Primer for Local Law Enforcement Agencies*, May 2013.

13. *** Los Angeles Police Department, *Report to the Board of Police Commissioners, An Examination of May Day* 2007.

14. *** *Managing Major Events: Best Practices from the Field*, Police Executive Forum, Washington, 2011.

15. *** Department of Defense, *Dictionary of Military and Associated Terms.*

16. *** *Joint Concept Note 2/17*, Future of Command and Control, Development, Concepts and Doctrine Centre, 2017.

17. *** *Public sector achievement in 36 countries. A comparative assessment of inputs, outputs and outcomes*, The Netherlands Institute for Social Research, The Hague, December 2015.

18. *** World Economic Forum, *The Global Risks Report 2020*, 15th Edition, In partnership with Marsh & McLennan and Zurich Insurance Group.

19. *** *Dicționar enciclopedic*, Editura Cartier, ediția a V-a, revizuită și actualizată, 2004.

20. *** *FBI Law Enforcement Bulletin*, octombrie 2019.

B.   Books, articles and web-sources

1. Thomas, Carothers and Richard ,Youngs — *The Complexities of Global Protest*, Carnegie Endowment for International Peace, 2015.

2. Manuel Castells — *Comunicare și putere*, Editura Comunicare.ro, 2013.

3. Cedric de Coning; Mateja, Peter — *United Nations Peace Operations in a Changing Global Order*, Palgrave Macmillan, 2019.

4. John, Christian; Matthew, Lewis; Scott, Gerwehr; Russell W. Glenn, Barbara R. Pantich, Dionne, Barnes-Proby; Elizabeth, Williams; David, Brannan — *Training the 21st Century Police Officer. Redefining police professionalism for the Los Angeles Police Department*, Public Safety and Justice RAND, 2003.

5. Marleen, Easton — *Military Policing, The Sage Encyclopedia of War: Social Science Perspectives*, Sage Publications; 2017.

6. Trevor, Findlay — *The Use of Force in UN Peace Operations*, Stockholm International Peace Research Institute, 2002.

7. Juan Carlos Montalvo Abiol — *Concepto de orden público en las democracias contemporáneas*, Revista Jurídica Universidad Autónoma de Madrid, nº 22, 2010-II.

8. Nathan, K. Finney, — *Mission Command in the 21st century: Empowering to Win in*

	Jonathan, P. Klug	*a Complex World*, Fort Leavenworth, Kansas, The Army Press, 2016.
9.	Nate, Huber	*Intelligence led policing for law enforcement managers*, in FBI Law Enforcement Bulletin, octomber 2019.
10.	Jaïr van der Lijn; Ivan, Briscoe; Margriet, Drent; Kees, Homan; Frans-Paul van der Putten; Dick, Zandee	*Peacekeeping operations in a changing world*, Netherlands Institute of International Relations Clingendael, 2015.
11.	C. Martellaa; J. Li, C. Conradob; A. Vermeerenc	*On Current Crowd Management Practices and the Need for Increased Situation Awareness, Prediction, and Intervention*, 2016.
12.	Tony, Narr; Jessica, Toliver; Jerry, Murphy; Malcolm, McFarland; Joshua, Ederheimer	*Police Management of Mass Demonstrations: Identifying Issues and Successful Approaches*, Police Executive Research Forum, 2006.
13.	Stephen, Otter	*Urban Safety Project, Urban Policing in Myanmar*, The Asia Foundation, October 2017.
14.	Marco, Sassòli	*Legislation and Maintenance of Public Order and Civil Life by Occupying Powers*, The European Journal of International Law, vol. 16 no.4, 2005, p. 665.
15.	Alexander J. Shackman; Richard J. Davidson	*The Nature of Emotion. Fundamental Questions*, Second Edition, Oxford University Press, 2018.
16.	Bernard, Stirn	*Ordre public et libertés publiques*, Intervention du 17 septembre 2015 lors du colloque sur l'Ordre public, organisé par l'Association française de philosophie du droit les 17 et 18 septembre 2015.
17.	Vladas, Tumalavičius; Jānis, Ivančiks; Oleksandr, Karpishchenko	*Issues of Society Security: Public Safety under Globalisation Conditions in Lithuania, Journal of Security and Sustainability Issue*, 2016 June Volume 5 Number 4.
18.	***	https://www.jcs.mil › Portals › Documents › Doctrine › pubs › dictionary.
19.	***	https://www.few.vu.nl/~cma330/papers/SafetyScience.pdf.
20.	***	https://www.statewatch.org/news/2010/nov/eu-policing-protests-godiac-project.pdf.
21.	***	http://www.jandarmeriaromana.ro.
22.	***	https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers.

23. ***   https://www.conseil-etat.fr/actualites/discours-et-interventions/ordre-public-et-libertes-publiques.
24. ***   https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers.

BREXIT – ŞI VIITORUL POLITICII EXTERNE ŞI DE SECURITATE COMUNĂ A UNIUNII EUROPENE

BREXIT – AND THE FUTURE OF EUROPEAN UNION FOREIGN AND COMMON SECURITY POLICY

Lieutenant Colonel, Lecturer Bogdan-Cezar CHIOSEAUA, PhD
Academia Forţelor Aeriene „Henri Coandă"
E-mail: b.chioseaua@gmail.com

__Rezumat:__ Uniune, alianţă, parteneriat, imperiu,… sunt termeni care din punct de vedere conceptual sunt diferiţi, însă atunci când ne raportăm la etape istorice, în care au avut loc aceste „coaliţii", observăm că toate au urmărit în principal acelaşi lucru. Puterea.

Dominaţie, supremaţie, deţinerea controlului total, termeni ce pot fi asimilaţi ca şi atribute ale puterii, analizaţi la nivel naţional tind spre o imagine a unei crude dictaturi, însă raportaţi la repere istorice, constatăm că, cel mai adesea acestea s-au instaurat prin violenţă şi prin subminarea puterii celui mai slab. Unele forme moderne ale războiului (Războiul Hibrid) ne demonstrează faptul că, mai nou, violenţa poate fi înlocuită de înşelăciune şi manipulare a maselor.

__Cuvinte cheie:__ Brexit, securitate. alianţă, uniune, referendum, Mare Putere.

__Abstract:__ Union, alliance, partnership, empire,… all of them are terms that are different, conceptually speaking, but when we refer to historical stages, in which these "coalitions" took place, we notice that they all pursued mainly the same thing. The power.

Domination, supremacy, total control, terms that can be assimilated as attributes of power, analyzing them at national level they offer an image of a cruel dictatorship, but compared to historical landmarks, we find that, most often they were established by violence and by undermining the power of the weakest. Some modern forms of warfare (like Hybrid Warfare) recently show us that, violence can be replaced by deception and mass manipulation.

__Keywords:__ Brexit, security, alliance, union, referendum, Great Power.

Introduction

On January 31st, 2020, at midnight, Great Britain left the grand European family after almost half a century of "cohabitation".

Europe's geopolitical map seems to be changing. England, an important actor on the Euro-political stage, and a main character when we are talking about Common Foreign and Security Policy (CFSP), is leaving the European Union (E.U.); yet, with the promise that it is not going to leave Europe too[1] but it is going to honor its commitments to the common security and defense of Europe.

Why has it come to this? Was the referendum on June 23rd, 2016 a surprise? Is Brexit an instance of hybrid warfare? And, more important, which are the effects that Brexit is going to propagate upon E.U.'s CFSP? All these are questions still to be heard on the hallways and in the meeting rooms of many European administrations.

In an attempt to find pertinent answers, there is a need for a brief X-ray regarding what the E.U was before and especially after the adherence of the United Kingdom.

Benchmarks

On March 25th, 1957, Belgium, Germany, France, Italy, Luxemburg, the Netherlands, members of the European Coal and Steel Community lay the foundation of an economic community, Economic European Community (CEE), the predecessor of nowadays' European Union, a structure, an „alliance" meant to bring an important contribution to the economic growth of member states through trade. In order to consolidate this „alliance", its founding members also launched in 1950 a project of constituting a European Community for Defense, a European army, initiative that was not successful, one of the reasons being the freshly founded alliance, North Atlantic Treaty Organization - NATO, that came with the mission of ensuring the protection of member states by political and military means.

One by one, in time, most European states joined the CEE. Nowadays, E.U., taking over CEE legacy, has 27 members that, all together, developed the old CEE and built a political and economic union which has a unique internal market, with a modern and standardized system of laws.

---

[1] Interview given by British Prime Minister Theresa May to *Bild* on 20th January 2018 *[https://www.   bild.de/politik/ausland/brexit/will-you-miss-us-mrs-may-54535638.bild.html]*, accessed on 02.04.2020.

Sixteen years after the constitution of CEE, on January 1st, 1973, the United Kingdom of Great Britain and Northern Ireland, courted many times and having gone through several failed adherence attempts, finally manages in spite of skepticism and doubts to join the European Community. The shadow of mistrust hovering over the continent referring to the economic incompatibility of United Kingdom as well as its reserved position when there were discussions about certain European projects[2] was never entirely gone even if the referendum in 1975 proved that over 67% of British people manifested their intention to stay within the European Union..

Thus, the United Kingdom joined the European family even if sometimes the directions imposed from Strasbourg, Brussels, and Luxemburg [3] were not exactly congruent with the Brits' opinions, a nation accustomed to being treated differently, from its position of great economic and military power, for which the European norms and rules, compulsory for other member states, were often subjects for debates and even disputes at Westminster[4].

London found it increasingly difficult to accept its position as "Member State" to the detriment of its statute of „Great World Power", and its priorities were represented by its national interest in preserving the island's unity (England, Scotland and Wales) and the major concern regarding improving the already privileged relations it shared with United States of America in the economic and especially in the military sector. Moreover, the political games and the confrontations between conservatives and labour representative[5] had new stakes – staying or not within the

---

2 The British Government refuses the implementation of European Monetary System. British Prime Minister Margaret Thatcher supports the importance of maintaining the sovereignty of Great Britain and expresses her reserve and even distrust in this European project, *[https://www.margaretthatcher.org/document/107332]*, accessed on 02.04.2020.
3 Strasbourg, Brussels and Luxembourg – The three joint capitals of Europe and premises of European Parliament, *[https://www.europarl.europa.eu/sides/getDoc.do...],* accessed on 02.04.2020.
4 The place where there are the two chambers of the Parliament of United Kingdom of Great Britain and Northern Ireland: House of Lords and House of Commons, *[https://www.parliament.uk/],* accessed on 02.04.2020.
5 Conservative Party – center-right political party, Labour Party – center-left political party – political parties in the United Kingdom famos for their rivalry

European Union – and, above all these, the migration crisis during 2015-2016 and the fact that United Kingdom, the second greatest European economy participates with important contributions to the European budget (approximately 9 billion pounds per year, the equivalent of 0.5% of country's GDP[6]) does nothing but loom the way of England outside the European Union.

So, the question "Why has it come to this?", though scientifically unacceptable, can be answered with a rhetorical question, namely "Did Great Britain really wish to be part of the European Union in the first place?". Taking into account also the aspects mentioned above, we may formulate a conclusion that maybe should have been anticipated by the decision makers in Brussels: United Kingdom and European Union are two entities which cannot be always compatible, especially when the issues at stake are national interests, economic and financial interests or political games.

Brexit and the British people's wishes

The idea of „Brexit" occurred relatively fast, given the moment when the United Kingdom adhered to the E.U., in 1973, when, through a legislative procedure proposed and supported by the conservative party in office at the moment, England became E.U. member state. The method used by the conservatives was vehemently contested by the labour government that, a year later, after taking over the power, deemed it as illegal and stated that for Great Britain to be part of the Union, British citizens had to be openly consulted. As a result, in 1975, the first referendum was organized regarding United Kingdom's belonging to the E.U., the labour party thus honoring their promises during the electoral campaign.

This is a period marked by changes and fluctuations of power relations and ratios. The political majorities in the Chambers of Westminster Palace keep changing due to the outcome of democratic elections, preceded by long prepared electoral campaigns which do not lack in populist speeches

---

[https://www.openpolitics.ro/conservatorii-si-laburistii-lupta-pentru-brexit/], accessed on 02.04.2020.
6 *https://business24.ro/international/ue/de-ce-vrea-marea-britanie-sa-iasa-din-ue-15649,* accessed on 02.04.2020.

glorifying the greatness of the British Empire and criticizing the fact that London's decisions became subject of scrutiny and analysis on the continent.

However, the first "attempted" Brexit failed. The electorate of the United Kingdom decides in a proportion of 67,2% remaining in the European Union showing, on the one hand, people's interest in the development and involvement in the common projects with European partners and, on the other hand, trying to maintain through this sense of belonging a way to influence and control a great center of power of the world.

The European Union is on a growing trend. Its development at all levels also implies implementing new common directions of actions, measures of coordination, monitoring, and control, all serving as grounds for elaborating packages of law and restrictive regulations. The great majority decides on adopting principles and systems that all European states need to get connected to.

Great Britain is put in a situation in which it has to accept the initiatives of European Unions, even if they are proposed by France or Germany.

The conservative position of the United Kingdom is starting to be quite uncomfortable and to feel so, when there is a decision regarding the implementation of a European Monetary System and, through the refusal to accept its implementation, England does nothing more than to confirm the fact that it is still tributary to the historic French-English rivalry, while the conditions and decisions made and imposed by „Brussels"[7] are increasingly hard to digest.

Under these conditions, a new attempt for a referendum seemed to become apparent. New parties emerged on the political stage of the United Kingdom, born out of the vehement desire to break free from the E.U., a desire that was so strong that one of the newly constituted parties received the name of their main objective „Referendum Party". It self-dissolved in

---

[7] British Prime Minister Margaret Thatcher's speech, held in Bruges in 1988 according to *[https://www.margaretthatcher.org/document/107332]*, accessed on 02.04.2020.

1997, the great majority of its members entering the ranks of another Euro-skeptical party, United Kingdom Independence Party (UKIP).

Despite all these, Great Britain keeps „surviving" within the Union, but, starting with the appointment on May 10th, 2010, of David Cameron as Prime Minister, things start to change.

Cameron gets the mission to create the first liberal-democratic governmental coalition after War World Two, a political alliance that the youngest Prime Minister in the last 200 years need to lead in the recently entrusted mandate. The period that follows is full of turmoil, from several points of view, both internally and externally.

Thus, internally, in order to preserve cohesion within the coalition, the English conservatives' leader launches promises and promotes ideas and opinions that he himself is not always entirely convinced of. Although the supports the idea that Great Britain should remain within the European Union, David Cameron proposes the government he is leading the organization of the referendum, thus giving in to the pressures of UKIP, led by Nigel Farage, a vehement supporter of Brexit.

Externally, the refugee crisis pressures both the E.U. and Great Britain, while, at European level, directions and measures are thought of, stipulating even the establishment of refugee shares for each individual state. These actions destabilize the labor market in the United Kingdom, reason for which Brussels' decisions are received with skepticism and virulent reactions in London, especially by pro-Brexit leaders who use this reason to draw on their side those who face difficulties in finding employment.

Under these circumstances, the result of the referendum is no longer a surprise. With 51,9% for Brexit, 72% of the British citizens decide the exit of United Kingdom from the E.U. and forces the government in London to assume all costs and especially the risks that Great Britain becomes exposed to given the acceptance and validation of the referendum result.

Briefly, Brexit, from the perspectives exposed above, was determined by two main causes: the lack of firmness of Cameron government and the refugee crisis overlapping the discontent of Great Britain middle class.

Brexit – a form of hybrid warfare

Analyzing the causes presented above and the manner in which they were propagated and disseminated towards the British population with the right to vote, we can notice the fact that a series of press trusts approached the Brexit issue both from as supporters of staying in the E.U. and from Euro-skeptical positions, against continuing the cooperation with the E.U., thus using the power of the press in order to influence the electorate.

Following this endeavor and analyzing mass-media's interest in Brexit, we cannot leave out an aspect which can be considered a threat to United Kingdom's national security system, namely the „bombing" of the public space with information transmitted through the press, social networks, or shows on radio and television stations. Thus, public political debates start to increasingly resemble „entertainment shows" in which the Union membership is approached in an ironical manner and positive aspects are presented as resulting from the possible breaking away from it.

Another aspect, extremely well known to those chasing fiscal paradises and in contradiction with the E.U. fiscal policy is the fact that Great Britain is renowned for being extremely permissive, not applying taxes on the outcome produced / gained outside the United Kingdom, fact which generated a real drift of a lot of billionaires in the world towards the British capital, with investments in domains such as real estate, media, sports etc.

Another fact worth mentioning is that the government in London and especially the Brits with a right to vote, did not seem in the least bothered by the presence of Russian oligarchs, Indian magnates, or billionaire princes coming from Arab states who make massive investments in real estate and, in order to ensure their accounts, purchase local and national publications or shares at the most important socializing platforms, and who end up sponsoring electoral campaigns.

Their presence in the most exclusive clubs and their acquisition of residences in the most expensive residential areas in London are not regarded with the same worries and concern as is E.U.'s proposition to assign a share of immigrants to the United Kingdom[8].

---

[8] London, in the autumn of 2015 turns down the assignment of the 17,000 share of refugees out of the total number of approximately 160,000, *[https://www. ziare.com/invazie-*

Huge amounts of money are poured forth in the British banking system, representing the capital infusions of immigrant investors, considerable sums not always and not entirely obtained through the cleanest, most honest methods.

The „cream" of Russian billionaires show great interest in British investments and among the „personalities" pertaining to this social category we cannot help but mentioning some of the most interesting characters, such as: Russian billionaire Alexander Lebedev – former KGB agent, that who buys the English publications „The Independent" and „Evening Standard"; Alişer Usmanov – important member in Gazprom leadership, that who invests in shares for Facebook and for the London football club Arsenal FC; the well-known Roman Abramovici – who has invested in natural resource businesses and who owns London football club Chelsea; Oleg Deripaska – the Russian king of aluminum, owner of luxury apartments in Belgrave Square and Surrey, who is actually close to President Vladimir Putin and at the same time a good friend of powerful political people in Great Britain, and the list may go on...

However, what results as obvious from the previous statements is the fact that, one way or another, through the coordination of political environments and by influencing the masses, the deed was done: United Kingdom was separated from the European Union. The main official reasons were political quiddities and the fear that Great Britain might „sink" under the flow of immigrants.

The real reasons are completely different in nature. Even if they seem to originate in a classical conspiracy theory, they are realities impossible to deny. The fact that a big power like Russia is sending its spies and potent businessmen in a country where they get to influence the political class and the electorate through ambiguous sponsorship and spectacular headlines in scandal papers can be interpreted as involvement in England's internal affairs.

The reason?

---

imigranti/stiri-invazie-imigranti/ presa-britanica-dezvaluie-planul-ue-romania-cota-de-7-000-de-imigranti-marea-britanie-nu-primeste-niciunul-infografic-1380816], accessed on 02.04.2020.

Keeping open one main commercial route and source of illicit money for a great power which for a long time was subject to the pressure of international sanctions and restrictive measures.

Thus, we may conclude by saying that Great Britain continues to be under siege and the malignant strikes of a hybrid war, a confrontation it is complacent with in order to cover the gaps in the Kingdom's treasury caused exactly by the decision to break away from the E.U. This is a confrontation which is highly unlikely to end soon, the last hope of the United Kingdom remaining its strong connection to NATO and United States of America.

Conclusions

With or without Great Britain, the European Union continues on its way. One of its main areas of interest remain the development of strategic thinking in the field of Common Foreign and Security Policy (CFSP) and in that of Common Security and Defense Policy (CSDP).

E.U.'s expansion towards the East of the continent, as well as the adherence of more Eastern European states to the North-Atlantic Alliance is creating a feeling of unrest for the Russian Federation whose reactions were those of consolidation in the Black Sea region, by annexing Crimea, and of impressing NATO and E.U member states, by naval maneuvers in Barents Sea[9] and Baltic Sea[10] as well as by air raids[11], at the border of national airspace.

The breaking of United Kingdom away from the European Union, also following the specific actions characterizing a hybrid warfare type of confrontation represents nothing but a battle won in the Union's struggle for a modern and powerful alliance from an economic and military point of view.

---

[9] Military exercise Zapad-2017, an actual simulation of a conventional war against NATO troops in Europe, *[https://www.hotnews.ro/stiri-international-22188277-manevrele-militare-zapad-...],* accessed on 05.04.2020.

[10] Military navy exercise Ocean Shield - 2019, *[http://www.paginade rusia.ro/marina-rusa-desfasoara-manevre-de-anvergura-in-marea-baltica/]*, accessed on 05.04.2020.

[11] *https://moldova.europalibera.org/a/rusia-violeaz%C4%83-spa%C8%9Biul-aerian-nato-pe-fundalul-manevrelor-din-estonia/30181312.html,* accessed on 05.04.2020.

The CFSP structure is nothing but putting together the policies of national security of member states. The directions of evolution for this structure aim at implementing a global strategy with an aim related to security and defense, in all its aspects, of state and societal resilience, integrated approach of external crises and conflicts as well as achieving regional order in a cooperative manner.

Although Great Britain has stepped outside the Union, it has not left Europe too, reason for which it is going to continue to participate in common CFSP projects, fulfilling the commitments already made and, for the future, on the basis of cooperation and collaboration agreements, it is going to remain a trustworthy partner in the Western European flank. The development of relations of cooperation is going to result in a renewed desire of the United Kingdom to be together again in a better and more powerful Europe.

References

1.	Rudolf G. Adam	*Brexit: Causes and Consequences*, Publisher: Springer, 2020.
2.	Thomas Christiansen, Diane Fromage	*Brexit and Democracy: The Role of Parliaments in the UK and the European Union*, Publisher: Springer International Publishing, 2019.
3.	***	https://www.bild.de/politik/ausland/brexit/will-you-miss-us-mrs-may-54535638.bild.
4.	***	https://www.margaretthatcher.org/document/107332.
5.	***	https://www.europarl.europa.eu/sides/getDoc....
6.	***	https://www.openpolitics.ro/ conservatorii-si-laburistii-lupta-pentru-brexit.
7.	***	https://business24.ro/international/ue/de-ce-vrea-marea-britanie-sa-iasa-din-ue.
8.	***	https://www. ziare.com/invazie-imigranti/stiri-invazie-imigranti/presa-britanica... .
9.	***	https://www.hotnews.ro/stiri-international-22188277-manevrele-militare-... .

INFORMAȚIA PENTRU APĂRARE ÎN CONTEXTUL CONFRUNTĂRII INFORMAȚIONALE

INFORMATION FOR DEFENSE IN THE CONTEXT OF INFORMATION WARFARE

Ion-Sorin MOLDOVAN, PhD candidate
E-mail: moldovan.ion.sorin@gmail.com

Rezumat: *Așa cum ne arată exemple relativ recente (cyber-atacul „OpIsrael" din 2013, atacurile cibernetice și informatice din același an din Singapore, agresiunile cibernetice din 2010, în Burma, Japonia și Coreea de Sud, cele din 2009, în SUA și Coreea de Sud etc.) în ultimii ani, operațiile militare menite să afecteze componenta militară a securității și care categorial se plasează în domeniul apărării, sunt desfășurate în multe cazuri prin utilizarea unor mijloace non-armate, cel puțin nu prin utilizarea armelor în înțelesul tradițional al termenului. Aceste schimbări sunt produse de mutațiile înregistrate de societatea modernă, în special din cauza evoluției tehnologice deosebite. Aceste evoluții au anulat de multe ori previziunile întocmite de mulți specialiști militari încă din perioada războiului rece, bazându-se pe concepțiile clasice. Autori precum Alvin Toffler[1] au sugerat totuși apropierea momentului în care se va dezvolta într-atât societatea informațională, încât însuși mediul de confruntare se va transfera de pe câmpul clasic de luptă în mediile virtuale ale câmpului informațional. Clipa în care informația a obținut o asemenea valoare, devenind totodată „scut" și „armă", a condus la conexiunea logică dintre situația controlului asupra informației și deținerea puterii. Astfel încât, în cadrul confruntării moderne duse într-un spațiu multidimensional, dimensiunea informațională a căpătat o importanță aparte. Rămâne așadar de văzut din perspectiva informației pentru apărare, cum se modifică „regulile jocului", în contextul generalizării confruntării informaționale.*

Cuvinte cheie: *informații, informații pentru apărare, mediu informatic, mediu virtual, rețele de calculatoare.*

Abstract: *As the relatively recent examples show us ("OpIsrael" cyber-attack of 2013, cyber-attacks of the same year in Singapore, cyber-attacks in 2010, in Burma, Japan and South Korea, in 2009, in the US and Korea South etc.), in recent years, military operations aimed at affecting the military component of security and being categorically*

---

[1] Alvin Toffler, Heidi Toffler, *Război și antirăzboi. Supraviețuirea în zorii secolului XXI*, Editura Antet, București, 1995.

placed in the field of defense, are carried out in many cases with the use of non-armed means, or at least not with the use of weapons in the traditional sense of the term. These changes are caused by the changes of the modern society, especially due to the special technological evolution. These developments have often cancelled the forecasts made by many military specialists since the Cold War, based on the classical concepts. Authors such as Alvin Toffler suggested, however, that the information society would develop in such a way that the confrontation environment itself would be transferred from the classic battlefield to the virtual media of the information field. The moment when information gained such a value, becoming "shield" and "weapon", led to the logical connection between the state of control over information and the holding of power. Thus, in the context of the modern confrontation in a multidimensional space, the information dimension has acquired a particular importance. Therefore, it remains to be seen from the perspective of defense information, how the "rules of the game" change, in the context of generalizing the information confrontation.

Keywords: information, information for defense, IT environment, virtual environment, computer networks.

Introduction

In the context of the multidimensional modern conflict[2], confrontation came to be transferred at a certain moment from the material environment to the information one, this fact having its specific influences upon the manner in which, currently, information for defense needs to be managed. The conflict taking place in the information age targets mainly information for defense and, in this regard, the forces sent into "battle" are those forces specialized in cyber and information actions, besides the more or less traditional information actions.

Such an unconventional confrontation shows us the information for defense that has become target and goal, but in a situation in which it can be used in an offensive or a defensive manner, as (counter)informative actions undertaken either independently, or within vast operations (usually conducted also in other dimensions of confrontation) which have as a purpose not only aspects related to the information environment, but, just as well, those connected to the psychological environment (psycho-sphere)and the interaction between human personnel and the information management equipment. The new types of operations (involving defense operations) are

---

[2] Gheorghe Arădăvoaice, Valentin Stancu, *Războaiele de azi și de mâine, agresiuni nonconvenționale*, Editura Militară, București, 1999.

conducted in such a manner that they also target the mental sphere of the enemy, looking as much as possible to avoid resorting to traditional fighting means and, generally, to activities conducted in a material, 3D environment. The combat for defending or attacking information for defense tends to be carried out in the information environment and, especially, in the IT or cyber one[3].

How does information confrontation affect the environment of information for defense?

At the present moment, the actions related to information confrontation are conducted in various manners[4], most often being directed towards certain categories of information, especially the information for defense which, usually, are considered to be very well-protected. Given the conditions of the multi-dimensional conflict[5], this protection of information for defense becomes increasingly difficult, especially as the new forms of confrontation can be occur as follows:

➢ As confrontations taking place at the *command/control echelon*; most often, these actions are also accompanied by traditional (classical) forms of combat, especially with respect to the modalities of target acquisition; these make up an important component of the confrontation undertaken in the information environment, most often based on modalities of using information in the military field, especially information for defense, when they are managed at C2l level[6];

➢ Within the *psychological confrontation*, by modifying the correct perception upon reality of the people that contribute to obtaining or processing data that represent the grounds for shaping information for defense; by influencing the psychological and moral state of the issuers of information for defense, the decision makers can be influenced in such a way so that success is achieved without resorting to violence;

---

[3] Stan Petrescu, *Arta și puterea informațiilor*, Editura Militara, București, 2003.
[4] Abram Shulsky, Gary Schmitt, *Războiul tăcut*, Editura Polirom, Iași, 2008.
[5] Constantin Moștoflei, Gheorghe Văduva, *Tendințe în lupta armată*, Editura Universității Naționale de Apărare, București, 2004.
[6] Mircea Mureșan, Gheorghe Văduva, *Războiul viitorului, viitorul războiului*, Editura Universității Naționale de Apărare, București, 2004.

➢ Under the deceitful appearance of a *virtual action*[7], usually to be found in the IT and/or cyber environment, through this action the virtual space is altered, thus creating fake images, the cyber or IT equipment belonging to the enemy, deceiving the enemy and thus allowing the alteration of the information for defense one way or another;

➢ As *propagandistic and imagological actions*, these coming together most of the time with psychological actions and usually having an indirect effect upon information for defense;

➢ Within the (radio)*electronic confrontation*[8] meant, usually, to destroy or alter the information flows that are transmitted through electromagnetic fields or which are stored in equipment influenced by the action of the induced electromagnetic field;

➢ As combat actions carried out in the *cyber* and the *IT* environment, the targeted ones being the enemy networks („*network warfare*"), which are subject to aggressions under different shapes, usually meant to prevent the processes of acquiring, undertaking, storing and processing data and information for defense by the enemy military networks (or those associated to them);

➢ Within the *media confrontation*, by influencing decision-makers with an important role in the management of information for defense as well as by creating false perceptions upon reality, resembling the manner in which actions are taken also in the propagandistic or imagological environments.

National defense is a domain of security in which it is absolutely crucial that data and information be correct, useful, and received by decision makers in real time. The technological advance of the last decades has led to the situation in which these operations are most often realized through IT and cyber means. It thus happens that the operations conducted in these dimensions (cyber, IT etc.) came to be directly of interest to information for defense.

---

[7] Maxim Dobrinoiu, *Infracţiuni în domeniul informatic*, Editura C.H. Beck, Bucureşti, 2006.
[8] Niculescu, Marian Mitea, Constantin Gh. Balaban, Gabriel Năstase, *Confruntările electronice şi psihologice - vectori de succes în conflictele internaţionale înalt tehnologizate*, Editura Victor, Bucureşti, 2003.

Targeting exactly information for defense, the enemy can conduct combat actions or even sequences of actions (operations) such as:

✓ Actions meant for acquiring classified data / information; the usual means of protecting information for defense prove many times inefficient in front of modern technologies that are increasingly sophisticated;

✓ Aggressions meant for the annihilation or even destruction of enemy networks[9] or rendering them impossible to use and, thus, preventing the access to information for defense stored there;

✓ Actions meant for preventing access to the network in case the network itself remains yet intact; thus, the issuers of information for defense may be prevented from delivering on time the information required by the users within the system of defense or the system of sensors that transmit this type of information, although functional, is no longer able to transmit it to the users as their access has been prevented;

✓ Actions meant to divert the usual directions and senses of activity of the networks through which the security information is managed, so that the users of these networks are sent (in the IT / cyber environment) in the wrong direction, either in order to intoxicate them or in order to delay their activity;

✓ One of the most encountered purposes is breaking codes or access codes and, thus, infiltrating in the enemy's networks without the enemy's realizing the respective action; certainly, information for defense is most directly targeted, given its importance in the equation of the confrontation, regardless the manner in which it is carried out;

✓ Aggressions that do not target directly either the enemy network or the senders of information for defense, but rather the actual content of data and information that gets at a certain moment to be perceived by the enemy and is capable of contributing to elaborating information for defense.

The future of information for defense

The aspects presented show us that in the context of the multidimensional environment of confrontation, information acquires both

---

[9] Tudor Niculescu, *Războiul electronic*, Editura Militară, București, 1991.

the role of target and of weapon[10]. As especially in the domain of defense information plays a paramount role, it is natural that within the information environment (with all its components) increasingly important effects may happen, regarding national defense. The combat actions specific to the information environment[11] tend to expand from the simple alteration of the information to the alteration of the mind frames of the people managing information for defense and influencing their decision-making capabilities in such a way so as to cause certain consequences upon the management of the information for defense and its efficacy.

The analysis of the present state of facts shows that the information confrontation targeting precisely the information for defense involve almost all the dimensions of modern confrontation.

Therefore, in the near future, *the networks in which information for defense is managed are going to be subject to specific risks* connected to the tendencies of technological development, as we perceive at present time. Thus, we might anticipate the following tendency of evolution of the situation regarding *information for security* in the context of modern confrontation:

✓ As the confrontation environment becomes multidimensional, the information for defense will need to develop according to all these coordinates, *acquiring specific shapes adapted to each dimension*;

✓ In case combat actions tend to continue to involve hybrid, unconventional (not necessarily NBC) and asymmetric means, their effects are not going to resemble the classical ones and the information for defense is going to have to adjust to new types of users – *a combatant personnel that is absolutely atypical*, capable to elaborate, process, and use information for defense in ways unconceivable for the previous generations of militaries or users of this kind of information;

✓ The counter-informative action regarding information for defense tends to affect environments or collectivities *which apparently have*

---

[10] Stan Petrescu, *Arta şi puterea informaţiilor*, Editura Militară, Bucureşti, 2003.
[11] Sorin Topor, *Războiul informaţional*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.

no connection to the users of information for defense; there are going to be more and more actions targeting the psychology of masses and collective masses, the influencing of information for defense becoming *indirect but no less efficient*;

✓ Directing aggression not only towards the information for defense or the personnel managing it, but also *upon the network*, to the purpose of deteriorating it and misleading the enemy decision makers.

Conclusions

Such tendencies lead to the necessity of reconceiving the manner of organization[12] of systems meant for managing information for security in any way possible and a change in even the general management of information for security, in the sense of adjusting to the new conditions imposed by the technological development.

Otherwise, we may find ourselves in a situation in which a potential enemy defeats us from a distance, without even being able to see his face and without[13] using violence in its classical forms.

References

1.	Arădăvoaice, Gheorghe; Stancu, Valentin,	*Războaiele de azi şi de mâine, agresiuni nonconvenţionale*, Editura Militară, Bucureşti, 1999.
2.	Dobrinoiu, Maxim	*Infracţiuni în domeniul informatic*, Editura C.H.Beck, Bucureşti, 2006.
3.	Marin, Ionel	*Comunitatea de informaţii, soluţia problemelor de securitate*, Editura ANI, Bucureşti, 2004.
4.	Moştoflei, Constantin; Văduva, Gheorghe	*Tendinţe în lupta armată*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2004.
5.	Mureşan, Mircea; Văduva,	*Războiul viitorului, viitorul războiului*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2004.

---

[12] Ionel Marin, *Comunitatea de informaţii, soluţia problemelor de securitate*, Editura ANI, Bucureşti, 2004.
[13] Sun Tzu, *Arta războiului*, Editura Antet XX Press, Bucureşti, 1993.

	Gheorghe	
6.	Niculescu, Tudor	*Războiul electronic*, Editura Militară, Bucureşti, 1991
7.	Niculescu, Tudor; Mitea, Marian; Balaban, Constantin Gh.; Năstase, Gabriel	*Confruntările electronice şi psihologice- vectori de succes în conflictele internaţionale înalt tehnologizate*, Editura Victor, Bucureşti, 2003.
8.	Shulsky, Abram; Schmitt, Gary	*Războiul tăcut*, Editura Polirom, Iaşi, 2008.
9.	Petrescu, Stan	*Arta şi puterea informaţiilor*, Editura Militara, Bucureşti, 2003.
10.	Sun Tzu	*Arta războiului*, Editura Antet XX Press, Bucureşti, 1993
11.	Toffler, Alvin; Heidi, Toffler,	*Război şi antirăzboi. Supravieţuirea în zorii secolului XXI*, Editura Antet, Bucureşti, 1995.
12.	Topor, Sorn	*Războiul informaţional*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2006.