"CAROL I" NATIONAL DEFENCE UNIVERSITY
Centre for Defence and Security Strategic Studies

P R O C E E D I N G S
INTERNATIONAL SCIENTIFIC CONFERENCE
STRATEGIES XXI

THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT

5th November, 2020

Editors
Florian CÎRCIUMARU, Ph.D.
Marius POTÎRNICHE, Ph.D.

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, ROMANIA

ISSN 2668-6511 (print); ISSN 2668-7828 (online)

C O N T E N T S

SECTION I
COVID-19 IMPACT ON SECURITY

SECTION II
SECURITY TRANSFORMATION

SECTION IV
STRATEGIC DEFENCE REVIEW – NATIONAL PERSPECTIVES

SECTION V
AREAS OF STRATEGIC INTEREST

DISINFORMATION AND THE PROTECTION POLICIES OF THE EUROPEAN CITIZENS

Rita PALAGHIA, Ph.D.
University Lecturer, Air Force Academy "Henri Coandă", Brașov, Romania.
Email: rita.palaghia@afahc.ro

Abstract: *The rapid global technological evolution, the deficit of training and endowment in the information field, the existent disagreement in social and political systems, the resources, technical solutions and the different means, make the EU a dysfunctional body, for the time being. Nevertheless, the European Union has proven to be the World's leader in adopting General Data Protection Regulation standards (GDPR). The next step of the EU Strategy is to structure public health policies, in conjunction with the protection of personal data. This generates differentiated types of actions for the State of Normality and the State of Emergency. The experience generated by the COVID-19 pandemic highlighted the need to accelerate the coordination of Common Security and Defence Policy and strategies at European level. The lessons learned after the "STUXNET" crisis, now followed by the "COVID-19 Pandemic" should convince us that the current situation has other valences and the chaos created by incompetence, lack of training, resources, clear and congruent plans and strategies can have dramatic effects on Humanity.*

Keywords*: COVID-19 pandemic; disinformation; European Policies; the State of Emergency; human rights; personal data protection.*

Introduction

The effects generated by STUXNET, Cambridge Analytica and other breaks through the security systems have highlighted the necessity to protect data of personal and National Interest having a clear legislative framework and standard acting procedures implemented in different crisis situations.

In the attempt to counter the most frequent cyber threats threatening the cyber security systems, EU adopted two strategies: *European Strategy for Internet Security – ESIS, 2011* and *Cyber Security Strategy for the European Union – EUCSS, 2013.* European Defense Agency - EDA and European Network and Information Security Agency – ENISA, together with a variety of national and other European structures, have been designated by the EU Parliament to facilitate the implementation of those strategies, having a key role in cyber defense and the security of information. Also for the protection of personal data and cyber security, in 2016 the European Council and the European Parliament have adopted EU Directive 1148 and EU Regulation 679.

Also in 2017 it has been established a new European Centre of Excellence for Countering Hybrid Threats (Cyber CEO), with an increased role in facilitating NATO and EU cooperation. In accomplishing those two responsibilities of the Centre, information gathering through EU Hybrid Fusion Cell–and combating online disinformation, Cyber CEO has contributed to the shaping of a clear situation generated by COV-19, but with a frequent violation of Human Rights and EU Policies, that cannot be stopped.

At the national level, in 2013 it has been adopted *Cyber Security Strategy of Romania* and the National Legislation has been adapted to EU requirements according to the reality and our own needs.

The Pandemic generated crises that had different global impact. Any crisis situation and/or an emergency situation have certain common elements and levels of analysis and action, depending on the existent information, the degree of trust in the sources of information and its rightness.

From the perspective of the subject in discussion and analysis, namely *Fundamental Rights*, more exactly the protection of personal data, the right to private life, security, equal treatment, personal opinion, of EU citizens, I focused my research on three directions for analysis:

a) The analysis of the way the information about COVID-19 and the means to counter the virus have been administered by different National and EU Channels;

b) The analysis of the way personal data has been collected „for the medical purposes" were used and if the EU Fundamental Rights in this respect have been violated or not;

c) The measures implemented by EU member states to counter disinformation.

The sources of those analyses were as follows: the provisions of the Charter of Fundamental Rights of the European Union monthly reports of the EU Agency for Fundamental Rights (FRA), studies and national reports published from the launch of the Pandemic mentioned in references. Additional to those we have the personal observations gathered from the public opinion reactions to the decisions of the National Crisis Management Cells and those of political actors.

The working hypotheses are as follows:

a) In crisis situations (State of Emergency or the State of Alert), the freedom of expression and information and the protection of personal data are frequently violated;

b) Disinformation is aggravating the perception level of a crisis and is reducing the population trust in state institutions.

1. "The viral Bomb" vs. fundamental rights

The initial data related to the dissemination mode, the morbidity index and the gravity in relation to other diseases were confused. At the beginning of February 2020, when the virus became a problem, the European States moved to the revision of National Plans for Emergency Situations and to impose or recommend limitation measures to spread the virus.

The results of the opinion survey conducted on-line in between 01st of Feb to 20th of March 2020, at the European level of the population (Italy, Spain, France and Germany) showed a massive public support for the restrictions imposed in the EU member states. 94% of the Austrian population that participated into the on-line survey conducted by Austrian Gallup Institute Barometer declared that is for the temporary renouncement to their civil rights in order to limit the spread of the disease[1]. In the United Europe the first signs of breaking its unity appeared, moving from the collective interest to the national one. National Governments decided to limit the effects of the virus based on the existent data and on the experience got in the actions related to crisis situations. Those decisions generated effects over the European Policies, especially on the Fundamental Rights specified in the Charter of Fundamental Rights of the EU. In bulletins no. 1 – 3 of Fundamental Rights Agency (FRA), are presented data gathered from the surveys, reports, official decisions of the EU states aiming at violating the violations EU citizens' rights, as follows:

[1] *Bulletin#1 Coronavirus Pandemic in the EU – Fundamental Rights Implications*, European Union Agency for Fundamental Rights (FRA), p. 12.

Table no. 1: Fundamental Rights violated in between 01.02-31.05.2020[2]

	B1 **01.02-20.03.2020** **Articles violated**	**B2** **21.03-30.04.2020** **Articles violated**	**B3** **01-31.05.2020** **Articles violated**
Measures impact on social life, education, education, work and justice system and travel to and within the EU	Art.2; Art. 35; Art.21; Art.6; Art.7; Art.10; Art.11; Art.12; Art.13; Art.45; Art.24; Art.14; Art.21; Art.27; Art.30; Art.34; Art.15; Art.16; Art.47	Art.6; Art.7; Art.10; Art.11; Art.12; Art.13; Art.45; Art.24; Art.21; Art.27; Art.30; Art.31; Art.34; Art.35; Art.15; Art.16; Art.47; Art.41; Art.20; Art.14(4) of the Return Directive	Art.45; Art.7; Art.12; Art.6; Art.13; Art.10; Art.11; Art.24; Art.14; Art.21; Art.27; Art.30; Art.31; Art.34; Art.35; Art.15; Art.16; Art.47; Art.41; Art.20; Art.41
Measures impact on particular groups in society (older, disabilities, Romma and Travelers, detainees, homeless persons)	National decisions in order to limit the spread of the contact and the freedom of movement	Art.25; Art.26; Art.1; Art.2;	Art.25; Art.26;
Incidents related to discrimination and xenophobia	Art. 21	X	X
Expansion of disinformation and of the effect of the isolation and quarantine measures over the protection of personal data and privacy; Apps and other technologies impact on FR (data protection and privacy)	Art.11; Art.7; Art.8	Art.7; Art.8;	X
States of Emergency or equivalent measures	X	Art.45; Art.12; Art.7	Art.45; Art.12; Art.7

From the beginning of the launch of the Pandemic, the European Council published a toolkit aiming information and the support of the Human Rights in EU member states.

1.1. Disinformation

The chaos created in the majority of the EU states, less Sweden manifested in the first three months have generated alienate behaviors and excessive restricted autocratic policies with serious violations of the Human Rights. By the end of March 2020, the population was

[2] *Idem* 2.

convinced of the necessity to respect the restrictive measures imposed by their National Governments but, disinformation that added the situational uncertainty has destabilized the trust of the population in the decisions taken by the state institutions on short and medium terms. Combating disinformation in EU countries has been achieved in a concerted way through public-private partnership. Some EU member states went further, establishing partnerships with searching engines and famous social media to counter disinformation and adding to their web pages some links to the official sites.

Representatives and governmental institutions through special designated mass media channels imposed a proactive communication with the population[3]. Germany, through their Chancellor (Angela Merkel); Sweden through the Minister of Defense; Austria, France, Hungary, Belgium, Estonia, Portugal, Poland, Lithuania, Romania (trough ministries and designated agencies) acted proactively to counter disinformation using official communicators. In Sweden, the governmental decision was that daily to have a press conference with the designated representatives of different national agencies. Slovakia, through their Interior Minister was very proactive in communicating with the citizens using Facebook. All the EU states established punitive financial measures to punish disinformation. With the purpose to understand the content of the official communication has been published/presented in different languages of international circulation and also using the sign language accessible for the deaf persons[4]. The Slovenian National Public Health Institute elaborated information packages for the blind persons[5]. Also, those efforts had deficiencies because isolated categories of persons, without any access to media channels or not knowing enough the communication language, did not get correct information. In order to overcome this aspect, mediators, specialized in health problems presented in those communities information related to symptoms and the prevention means/ways and explained why those excessive regional isolation measures are taken.

Under "the provision of the State of Emergency", some EU states introduced major punishments for the attempt to induce panic and for disinformation. For example, Hungary has introduced in Penal Code the punishment of one to five years in prison for the crimes related to disinformation. Denmark has introduced also in the Penal Code (Section 8_{1d}) severe punishments for crimes related to COV-19, including blocking the Web-sites. Those provisions are severe violations of the freedom of speech.

1.2. The protection of personal data

We will present in brief the level of knowing the rights regarding personal data protection of the EU population before the pandemic aiming to understand the exposure degree to the risks involving the mismanagement of those. In October 2019 EU Agency for Fundamental Rights accomplished survey[6]using 35,000 EU citizens older than 16 years old. They aimed to highlight the degree in which the Smartphone users are familiarized with their rights in relation to those (data protection, equal treatment, the access to justice, etc).

More than half of responders would be willing to share basic personal data with public administration, including their home address (63%), date of birth (62%), and citizenship (58%). Significant smaller percentages of the same users of data are willing to provide that information to the private companies. The results obtained show a limited knowledge of the rights related to the protection of personal data.

[3] *Idem* 2, p. 38.
[4] *Bulletin#1 Coronavirus... op.cit.,* European Union Agency for Fundamental Rights (FRA), p. 39.
[5] *Idem* 5, p. 39.
[6] *Idem* 12, pp. 42-44.

The next attempt conducted by EU Agency for Fundamental Rights after publishing the results of the survey mentioned before was to conduct another two in support of European Commission's new Security Union Strategy 2020-2024 and the elaboration of the EU Commission Report related to the application of General Rules for the data protection. For that purpose have been conducted the following opinion surveys: *FRA – Your Rights matter: Security concerns and experiences*[7]*and FRA – Your Rights matter: Data protection and privacy*[8]. Those have been conducted by Ipsos MORI in cooperation with Statistic Netherlands, the Centre des Technologies de l'information de l'Etat and Statistic Austria, and with the participation of 35000 persons older than 16 years old, different genders/occupations, from all EU member states. The results of those surveys covered only the cyber security aspects and personal data protection issues and are providing a comprehensive set of comparable data related to peoples' opinion about fundamental rights (data protection, equal treatments, good governmental administration, etc.). The majority the EU citizens manifesting serious concern regarding personal data protection (persons, Foreign Governments, International Organizations) used for illegal purposes or without permission[9].

On this relative knowledge and problems related to the obey of the Fundamental Human Rights basement, the crisis generated by COVID – 19 worsen the existing situation. In emergency situations, both General Data Protection Regulations (GDPR) and ePrivacy Directive are allowing certain flexibility in the adoption and implementation of the legislation related to the protection of personal data. In accordance with the article 23(1) of the GDPR, for reasons related to access to public health and personal data related to this can be approved with legal restrictions. The protection of the vital interests of the Community, generated by unexpected exceptional situations, is allowing the access to the personal data of the users of the mobile networks, but any violation of the freedoms and fundamental rights have to obey the principles of necessity, proportionality and legality and have to be temporary[10]. In a State of Emergency generated by a pandemic has been clearly understood that some personal data were to be collected aiming to elaborate a more correct profile of the groups that were presenting a high degree of risk to become sick and the surveillance of those being isolated and in quarantine The International institutions such as Global Privacy Assembly[11], the European Data Protection Board[12], the Council of Europe[13]and National Institutions that are regulating the protection of data ensured that everything will be obeyed when data are to be collected and stored for a longer period of time. Despite all those provisions the majority of EU member states asked for additional clarifications related to different aspects of the protection of personal data[14].

A controversial aspect related to the collection by some institutions or/and employers of personal data related to the associated diseases, symptoms, medical information collected

---

[7] *Your rights matter: Security Concerns and Experiences*, European Union Agency for Fundamental Rights (FRA), Fundamental Rights Survey, Luxemburg, Publication Office of the European Union, 2020.
[8] *Your rights matter: Data protection and privacy*, European Union Agency for Fundamental Rights (FRA), Fundamental Rights Survey, Luxemburg, Publication Office of the European Union, 2020.
[9] *Idem* 20, pp. 17-18.
[10] *CJEU*, Joined cases C-203/15 and C-698/15, Telez Sverige AB v.Post-ochtelestyrelsen and Secretary of State for the Home Department v. Tom Watson & Others, 21st of December 2016, paras. 98-102, 115, 125 and operative part.
[11] ***, "Statement by the GPA Executive Committee on the Coronavirus (COVID-19) Pandemic", *Global Privacy Assembly*, 17th of March 2020.
[12] ***, "Statement on the processing of personal data in the context of the COVID-19 outbreak", *European Data Protection Board*, 19th of March 2020.
[13] ***, "Joint Statement on the right of data protection in the context of COVID-19 Pandemic", *Council of Europe*, 30th of March 2020.
[14] *Bulletin#1 Coronavirus...*, *op.cit.*, p. 41.

by persons with or without any medical training have generated major concerns among the population and even the refusal to collect them. The evidence collected by FRA[15]from EU states showed that some states (Belgium, Estonia, France, Hungary, Italy, Luxemburg and Nederland) the collection of data related to the symptoms could be achieved only with the voluntary approval of the person. In other states if the collection is becoming a necessity, this is allowed in states such as Denmark, Finland, Germany, Italy, Lithuania, Poland, Slovakia and Spain).

In some European states such as Belgium, Finland, Ireland, Lithuania, Luxemburg and Nederland, identification of the infected persons has not to be made known and is also allowed to notice the working colleagues about the fact that a member of the personnel of the institution/organization is tracked positive. In other states such as (Denmark, Finland, Italy or Spain), the employer has the right to make known the identity of the person tracked positive.

1.2.1. Contact tracing apps

In March 2020 WHO asked the countries to test and monitor the persons with COVID-19 symptoms. This is reflected in the Joint European Roadmap towards lifting COVID-19 containment measures adopted by the European Council and the European Commission[16] that initiated discussions with telecommunication operators concerning the analysis model to use the personal data of the users without violation of the Fundamental Rights. The result of those discussions materialized in the development of some applications aiming to locate, collect and analyze personal data related to the Pandemics. The analysis of the data collected is supporting the detection of some patterns of the social mobility and based on that to elaborate predictions on the spread of the disease.

The implications of using those over the Fundamental Rights are major ones. Personal data, the right to privacy, the freedom of speech, the freedom of association, of using religious practices and the discrimination are only some of the right violated by the usage of those technologies. *Downloading and using of apps must always be entirely voluntary, the free choice of each individual*[17]. The wrong collection and interpretation of the data can activate prejudices on this data and social inequity. Also, it can worsen the social exclusion of those that are not benefitting of mobile technology or other forms of technology. But only a small part of those applications have been implemented because of the wrong legal definition of their usage.

A study conducted by the University of Oxford revealed that concluded data can be obtained only if more than 60% of the population is using health apps[18]. In most Member States, contact tracing apps used Bluetooth proximity data but in some countries apps used location data[19].Some applications stored local data users and others in central servers, raising the possibility to access unauthorized those. Some apps allowed the users to communicate with the medical authorities and others allowed the collation of this data outside the area of specialization of the receptor. All those details raised question marks over the transparency of collation, dissemination, period of storage and the way of encryption of this data. Much of this data have been put at the discretion of the Police in order to locate persons with medical problems and to check the degree of obeying the quarantine measures imposed.

---

[15] *Idem* 10, p. 42.
[16] *Coronavirus Pandemic in the EU – Fundamental Rights Implications: with a focus on contact- tracing apps, Bulletin#2,* FRA, ISBN 978-92-9474-959-8, Luxemburg, April 2020, p. 41.
[17] *Idem* 13, p. 5.
[18] *Digital contact-tracing can slow or even stop coronavirus transmission and ease us out of lockdown*, University of Oxford, 16 April 2020.
[19] *Idem* 12, p. 12.

The use of drones in order to check the obeying of the imposed distances, the usage of thermal detectors, imposing different documents in case of movement, etc. are representing severe violations of the Fundamental Rights related to the access of the personal information.

The on-line learning process is confronted with the same problems related the protection of data and cyber-security issues. Sweden, Nederland and Italy noticed that since the implementation of the on-line learning the security issues asked for guidelines from the Cyber protection national structures[20].

One of the most severe aspects related to the personal data protection is linked to the fact that the majority of the EU member states have been encouraged by the authorities for the collection of data[21]. Some countries like Austria, Greece, Hungary, Bulgaria and Slovakia have elaborated list with patients identified as being positive infected or dead with complete data. Others like Slovenia, Greece or Hungary have transferred lists in between several institutions. Slovakia, Portugal and Romania[22], made public personal data through different media channels.

1.2.2. Apps and fundamental rights standards

On 16th of April 2020, the European Commission – in Communication from the Commission, Guidance on Apps supporting the fight against COVID-19 Pandemic related to data protection[23], stipulated: *the functionalities included in the apps can have different impact on a wide range of rights enshrined in the Charter of Fundamental Rights of the EU, such as human dignity, respect for private and family life, protection of personal data, the freedom of movement, non-discrimination, freedom to conduct a business, and freedom of assembly and of association.*

On the European level beside EU Commission that published EU Toolbox si Guidance on Apps, numerous organizations published guides to support the governmental activity of the companies. Thus, European Data Protection Board (EDPB), EU Council elaborated a Joint Statement with directory lines and the Organization for Economic Co-operation and Development – OECD, are main contributing forums in guiding the actions related to apps. Both national organizations and international ones responsible for personal data protection showed concerns about the way and the period of time to store the data.

On 30th of April 2020 contact-tracing apps were already available, but the majority of the EU member states do not have specific legislation for the protection of the data introduced in contact-tracing apps. Only Belgium, Finland and France are preparing regulatory laws for the regulation of those apps. Anyway, the EU Parliament[24]proposed the usage of the decentralized model for a better storage and collection of personal data.

Romania, together with Greece, Hungary, Luxemburg, Sweden and Slovenia is from the few EU member states that do not have applications related to the location monitoring of the persons with COVID-19 symptoms. From the published data analysis, the most exposed country from this perspective is France.

The same problems are applied when we discuss about apps that are collecting and are collating only medical data. The lack of a certain and complete legislation, insufficient encryption, the lack of the security and usage of this kind of data are impediments that are

[20] *Idem* 20, p. 56.
[21] *Idem* 20, p. 56.
[22] ***, *Publishing personal and sensitive data*, The Group of NGO's for Democracy, Romania, 21st of April 2020.
[23] *Communication from the Commision, Guidance on Apps supporting the figh tagainst COVID-19 Pandemic in relation with data protection*, C92020)2523 final, European Commission, Brussels, 16th of April 2020, p. 4.
[24] ***, "EU coordinated action to combat the Covid-19 Pandemic and its Consequences", Resolution, (2020/2616(RSP)), European Parliament, 17th of April 2020, para. 52.

endanger the EU Fundamental Right of the EU citizens. Health reporting apps and websites exists in Slovenia, Italy, Germany, Spain, Croatia, Bulgaria, Greece and Denmark. In Sweden the existent applications has temporary stopped their functioning because of the irregularities related to data administration[25].

2. Case Study – Germany, Sweden and Romania in the COVID-19 pandemic

Trying to prioritize individual or group interest is a paradox and the public debate on this topic has not reached a generally accepted consensus. The issues of securing personal data and combating misinformation have been approached differently by EU member states. The main lesson learned so far from the COVID-19 pandemic is that, after the initial shock there is the availability to an extensive cooperation between EU member states.

Table no.2: Data protection and disinformation in crises generated by COVID -19 Pandemic in Germany, Sweden and Romania

GERMANY (a study conducted by *Deutches Institute fur Menschenrechtee*.V., published on the 02nd of July 2020)[26]	In March 2020 DEU Bundestag declared „epidemic situation of national relevance". (In German Constitution there is no provision related to the "State of Emergency". **Personal data and Apps** The most frequent subject in the data protection domain is represented by the location surveillance and monitoring approved by the Federal Government aiming the limitation of the spread of the disease. Until the data when the study has been published appx. 13 millions of citizens voluntarily downloaded the application via Bluetooth, with data collection facility[27]. **Spread of disinformation online** This is remaining a major problem, 80% of the population has declared that the news promoted by mass media is confused and are inducing panic. The Federal Government acted to counter the fake news through: the creation of a podcast, publishing several articles, by presenting the situation by a speaker, through the collaboration with civil organizations and the identification and fining the disinformation.
SWEDEN (study conducted by *Emerga Institute*, published on 02nd of July 2020)	The Constitution of Sweden (similar to that of Germany) does not comprise the provision of the declaration of the State of Emergency. The emergency measures that are to be implemented during the infectious pandemics are stipulated in „The Communicable Diseases Act". On 16th of April 2020 the Swedish Parliament adopted some amendments to this act, which gave the Government the power to introduce provisions considered very urgent that cannot wait the approval of the Parliament. The only right restricted in the context of COVID – 19 was the freedom of assembly for groups larger than 50 persons. All the other restrictions were recommendations without the right for the Police to impose or sanction them. **Personal data and apps** Ministry of Finance and the Ministry of Health and Social Affairs, made huge investments in the testing capacity and infectivity tracing (5,9 billion SEK, appx. 562.694.000 Euro).[28]

[25] *Idem* 20, p. 54.
[26] *Coronavirus pandemic in EU - Fundamental Rights Implications*, European Union Agency for Fundamental Rights, Germany, 2020.
[27] *Idem* 30, p. 14.
[28] *Coronavirus pandemic in EU- Fundamental Rights Implications*, European Union Agency for Fundamental Rights (FRA), p. 5, Sweden, 2020.

	Data Protection Authority has stipulated clearly the conditions in which personal data can be collected and the way they can be used, thus: a) data about an infected person have to be considered medical data; b) Information about a person coming back home from risk zones are not medical data; c) information about a person is working from home is not a medical data, only if he/she is infected with Covid-19; d) information about a person in quarantine is representing medical data; e) Personal medical data are considered sensitive information.[29] Personal medical data and the way they are administered are the responsibility of the Swedish Data Protection Authority and the Swedish Post and Telecom Authority. The researchers from the Lund University have declared the launch of an application, COVID Symptom Study on the 30th of April 2020, developed in UK aiming to show the location and he Covid dissemination (spread), based on the voluntary individual declared symptoms. To the ambiguity of the implementation of this application are added the problems generated by the content of the personal data protection policy. It is a strongly contested application[30] (Civil Rights Defenders, the Pirate Party, Association for digital Freedom and Rights)and very controversial, approved by the Ethical Review Authority[31]. **Spread of disinformation online** The fight against disinformation conducted by the authorities together with the Civil Society (Swedish Civil Contingencies Agency, Krisinformaton.se, Digiteket, the Swedish Internet Foundation, Sweden's Educational Radio, the Swedish Media Council, the Workers' Education Association, 8sidor.se, Hello Consumer, etc.) is one very efficient and attractive.[32]
Romania	At the 11th of March 2020, WHO declared the Pandemic and Romania, according the art. 15 of the European Convention on Human Rights (ECHR) got derogation from obeying some provisions for the State of Emergency, motivating the legality, the proportionality and the necessity of implementing some measures that are violating those provisions. **Personal data and Apps** Articles 10 and 13 from the Charter have been the first ones violated but Romania already got a temporary permission to disobey them in connection to the Fundamental Human Rights of the citizens and the imposed State of Emergency. In Romania, despite the general line to respect the identity of the sick person, mass-media made a purpose in an aggressive broadcasting of those cases. Our country was in between few EU member states that have no related applications in monitoring the location and the symptoms of the infected persons with COVID-19. **Spread of disinformation online** Romania (through the ministries and designated agencies) has proactive act to counter disinformation through official statements. The State through the Ministry of Internal Affairs based on the declaration of the State of Emergency decides to suspend the access or the on-line functioning license of the channels that were promoting disinformation[33].

[29] *Idem* 32, pp. 16-17.
[30] *Idem* 32, pp. 21-22.
[31] *Idem* 32, p. 20.
[32] *Idem* 32, pp. 22-24.
[33] *Report about COVID-19 Strategic Communication Group – A proposal to disable*, Ministry of Internal Affairs, Romania, 18th of March, 2020, URL: https://stiridemoment.ro

Conclusions

The response to the Pandemic, with respect to the obeying and circumvent of the provisions of the Fundamental Human Rights Charter of the EU citizens has been achieved in different ways in the EU member states. The main concern in the initial phase was to limit the effects generated by the COVID-19 Pandemic. Cooperation in between the State Institutions, International Organizations, monitoring mechanisms and the full range of human rights international actors can guarantee the preservation of the fundamental rights within the accepted limits during the State of Emergency.

The analysis of official documents together with the Case Study is entitles to state that both hypotheses presented in the introduction are confirmed.

The lessons learnt from the Pandemic are as follows:

- There is no perfect model that is to be applied by all EU member states;
- The measures implemented by the governments in crisis situations are to be according to the scale of risks and threats, they are to be temporary with the obey as much as possible of the Fundamental Human Rights;
- Public Policies in the medical and personal data protection domains have to be updated continuously;
- Social Policies implemented in crisis situations are not to affect vulnerable groups.
- The lessons learnt from the previous similar situations (Sweden) have generated policies and Standard Operational Procedures. The lack of clear legislation, clear institutional responsibilities, paying an active attention by the Officials to the civil institutions, on which we can add a studied nation's specific socio-cultural structure have facilitated the obey of the citizens' Fundamental Rights and the limitation of the Pandemic;
- The implementation of the standard acting procedures, the human and material preparation and the conjugated EU acting policies are efficient solutions for this type of generated crises.

BIBLIOGRAPHY:

1. ***, "EU coordinated action to combat the Covid-19 Pandemic and its Consequences", Resolution, 2020/2616(RSP), European Parliament, 17th of April 2020.
2. ***, "Joint Statement on the right of data protection in the context of COVID-19 Pandemic", *Council of Europe*, 30th of March 2020.
3. ***, "Publishing personal and sensitive data", *The Group of NGO's for Democracy*, Romania, 21st of April 2020.
4. ***, "Statement by the GPA Executive Committee on the Coronavirus (COVID-19) Pandemic", *Global Privacy Assembly*, 17th of March 2020.
5. ***, "Statement on the processing of personal data in the context of the COVID-19 outbreak", *European Data Protection Board*, 19th of March 2020.
6. *Bulletin#1 Coronavirus Pandemic in the EU- Fundamental Rights Implications*, European Union Agency for Fundamental Rights (FRA).
7. *Bulletin#2, Coronavirus Pandemic in the EU - Fundamental Rights Implications: with a focus on contact- tracing apps* (FRA) Luxemburg, April 2020.
8. *CJEU*, Joined cases C-203/15 and C-698/15, Telez Sverige AB v.Post-ochtelestyrelsen and Secretary of State for the Home Department v. Tom Watson & Others, 21st of December 2016.
9. *Coronavirus pandemic in EU - Fundamental Rights Implications*, European Union Agency for Fundamental Rights(FRA), Germany, 2020.
10. *Coronavirus pandemic in EU - Fundamental Rights Implications*, European Union Agency for Fundamental Rights (FRA), Sweden, 2020.

11. *Digital contact-tracing can slow or even stop coronavirus transmission and ease us out of lockdown*, University of Oxford, 16 April 2020.
12. *Guidance on Apps supporting the fight against COVID-19 Pandemic in relation with data protection, C92020)2523 final, Communication from the Commision*, European Commission, Brussels, 16th of April 2020.
13. *Report about COVID-19 Strategic Communication Group – A proposal to disable*, Ministry of Internal Affairs, Romania, 18th of March, 2020, URL: https://stiridemoment.ro
14. *Your rights matter: Data protection and privacy*, European Union Agency for Fundamental Rights (FRA), Fundamental Rights Survey, Luxemburg, Publication Office of the European Union, 2020.
15. *Your rights matter: Security Concerns and Experiences*, European Union Agency for Fundamental Rights (FRA), Fundamental Rights Survey, Luxemburg, Publication Office of the European Union, 2020.

THE IMPACT OF COVID-19 ON MILITARY POWER IN THE INDO-PACIFIC REGION

Florin DIACONU, Ph.D.
Associate Professor, Faculty of Political Science, University of Bucharest (FSPUB), Romania. E-mail: florin.diaconu@fspub.unibuc.ro

Abstract: *A few decades ago, John Naisbitt was openly listing a new major trend, already visible at that very moment on the international arena: the complex realities in the Pacific Ocean area were already massively important, and their global relevance grew larger and larger. Nowadays, this megatrend is even more important, leading both various political actors (leaders, states, political parties) and various analysts to an obvious conclusion: the Indo-Pacific region is the new center of the global system. In such a situation, the study explores, with some relevant details, the way in which the ongoing COVID-19 pandemic impacted the armed forces (military power) of some of the most important states in the Indo-Pacific region (mainly the US, China, India and Russia, but also some regional great powers – Japan, South Korea, Australia, and other regionally significant powers – Vietnam, the Philippines, Pakistan, Indonesia, and Taiwan, among others).*

Keywords*: Indo-Pacific region; military power; military forces; world powers; great powers; regional powers; COVID-19 pandemic; resilience; risks.*

Along several millennia, the very 'center of the world' – the very important region where most important political, military, economic and cultural events took place, and where most important trends emerged – was the Mediterranean, and then, starting with Late Middle Ages, the Atlantic. More recently, the location of the center of the world is swiftly gliding to the Indo-Pacific area. Such a trend was already visible in the late 1980s, when John Naisbitt was openly speaking about the "century of the Pacific"[1]. More recently, important authors in the field of International Relations and Strategic Studies have also offered clear opinions regarding the increasingly important role of the Indo-Pacific region. Even more recently, the United States, at this moment the only fully operational superpower on the international arena, decided to transform the Pacific Command into the Indo-Pacific Command; this decision is a clear proof of the effort made by U.S. decision makers to adapt the strategic posture of their country to quick and massive changes on the world arena. In this context, we are to seriously take into account the basic fact that the Indo-Pacific region is now concentrating an exceptionally large number of world powers and great powers[2], some of them clearly significant active geostrategic players[3] on the international arena, both at regional and global level.

[1] A.N.: For all these, see John Naisbitt, Patricia Aburdene, "Zece noi direcții pentru anii '90", *Anul 2000 – Megatendințe*, Humanitas, București, 1993, pp. 189-190.

[2] A.N.: For better understanding the way in which states can be classified, taking into account the magnitude and relevance of their power resources, and the role they play on the international arena, see, for example, Martin Wight, *Politica de Putere*, Ed. Arc, Chișinău, 1998, pp. 31-88 (chapters dealing with powers, dominant powers, great powers, world powers, minor powers, maritime powers, continental powers).

[3] A.N.: Dealing with the problem of the role(s) political actors are playing on the international arena, some important authors are openly stating some statens are geostrategic players (able to promote theirs interests by

Dealing with the impact of the COVID-19 pandemic on the military institutions and structures in the Indo-Pacific region (probably the most important, geo-strategically, in the entire world), we managed to identify *three major topics to be dealt with* by this paper, with some details and illustrative examples: 1. use of military forces in order to cope with the COVID-19 pandemic; 2. the impact of COVID-19 on the military manpower resources; and 3. the impact of COVID-19 on military activities (on quite many occasions, strategically significant) of all sorts.

1. Use of military forces, in order to cope with the COVID-19 pandemic

Different segments of military forces have been extensively used in the region, practically by all countries, both great and small powers, actively searching to accomplish several goals, connected in a way or another with the ongoing pandemic.

Monitoring the pandemic, delivering intelligence, forecasts. Let us not forget, for example, it was a Canadian *military* unit (belonging to military intelligence, as far as we know) that offered the first serios set of data on COVID-19, warning the Canadian authorities as early as January 2020: "A small, specialized unit within the Canadian military's intelligence branch began producing detailed warnings and analysis about the emergence of the deadly novel coronavirus in Wuhan, China in early January, CBC News has learned"[4]. The media source we are quoting here from is also reporting "the medical intelligence (MEDINT) cell within Canadian Forces Intelligence Command (CFINTCOM) is tucked away on the edges of the country's security and defence establishment. It has a mandate to track global health trends and contagion outbreaks to predict how they'll affect military operations…"[5].

Augmenting civilian resources and activities, in fighting against the consequences of the pandemic: In many of the countries of the region, military forces were asked to directly involve themselves, in different ways, in the effort against the pandemic. In *China*, for example (the country in the region which was massively hit by COVID-19, from the very beginning), all sorts of military institutional structures were directly responsible for "the transport to Wuhan of more than 4,000 military medical personnel" (from almost 20 large cities and all branches of the armed forces)[6]. Until early May, the PLA Air Force had organized airlift missions to the city of Wuhan, "involving 30 flights by Ilyushin Il-76 *Candid* and *Xian* Y-20A heavy transport aircraft, with *Shaanxi* Y-9 medium transport aircraft carrying both medical personnel and supplies. Additionally, some 200,000 militia drawn from 28 military districts, as well as more medical personnel and supplies, were brought in via bus and high-speed rail"[7]. *India*: as early as the end of March, *The Diplomat*, a very serious magazine focusing on Asia-Pacific, was reporting "the Indian Army has started training personnel to participate in assisting state authorities in enforcement efforts", also adding "India's lockdown, affecting some 1.3 billion people", was, at that moment, "the

means of actively using various means and political-military tools on the international arena), while other states do not have either the resorces or the will to do this, being in the end just territories where the politics will of the players is put to use – see for example Zbigniew Brzezinski, *Marea tablă de șah: Supremația americană și imperativele sale geostrategice*, Univers Enciclopedic, Bucharest, 2000, pp. 53-61.

[4] Murray Brewster, "Canadian military intelligence unit issued warning about Wuhan outbreak back in January", *CBC*, April 10, 2020, URL: https://www.cbc.ca/news/politics/coronavirus-pandemic-covid-canadian-military-intelligence-wuhan-1.5528381, accessed on august 21, 2020.

[5] *Ibidem*.

[6] Meia Nouwens (Research Fellow for Chinese Defence Policy and Military Modernisation), *China's armed forces and the impact of COVID-19*, on the webpage of the *IISS*, URL: https://www.iiss.org/blogs/military-balance/2020/05/china-armed-forces-covid-19-pla, accessed on August 25, 2020.

[7] *Ibidem*.

largest national policy response of its type to the ongoing pandemic in the world"[8]. The same source was also stating "the Indian Army has started training troops on how they might collaborate with law enforcement authorities to make sure that lockdown rules are followed… a major part of the training involves the type of equipment they need to carry, clothing to be worn and precautions to be taken for themselves and in treating and helping" citizens and communities[9]. In the *United States*, in the early stages of the pandemic, *large hospital ships of the U.S. Navy were deployed to large cities*, both on the East and West coasts: "public excitement and relief greeted the March arrival of the Navy's hospital ships in Los Angeles and New York City for their COVID-19 relief mission". One of them, "USNS *Mercy* (T-AH-19) left the port of Los Angeles on May 15 after treating only 77 non-infected patients"; and "the Norfolk, Va.-based USNS *Comfort* (T-AH-20) had returned to Virginia two weeks earlier after treating 182 patients in its month in New York City", *United States Naval Institute News* is reporting[10]. In *Australia,* authorities started deploying troops in Victoria (one of the Australian states), in June, in order to "cope with a sharp rise in coronavirus cases"[11]. On that occasion, media was reporting, "one thousand Australian troops" started boosting "security at quarantine facilities for travelers returning from overseas"[12]. The military also helped "with testing as the state struggles with a surge in COVID-19 cases"[13]. In the *Russian Far East*, on the shores of the Pacific, military medical teams belonging to the Russian Navy (Pacific Fleet) were deployed, in June 2020, to Kamchatka: "In accordance with the request of the leadership of the Kamchatka territory to the command of the Eastern Military District, it was decided to send an additional two medical and nursing teams of the Pacific fleet to medical institutions in the region to provide specialized assistance to civilian doctors in the treatment of infectious patients. The teams include specialists who were trained at the Kirov Military medical Academy on the treatment of a new coronavirus infection", the official media outlet of the Russian Ministry of Defence was reporting[14]. In *Latin America*, many troops are deployed, mainly in cities, to augment the ability of authorities to cope with the pandemic. This is the situation in several countries on the shores of the Pacific, countries to be regarded as *small or medium sized regional powers* – Peru, Chile, Colombia, Ecuador, Mexico. In these countries, "soldiers are present in the region's streets far more than before, enforcing lockdowns and curfews, either alongside police or on their own", and "pandemic-related security duties include patrolling, manning checkpoints, sealing borders, and in many cases detaining violators" of stay-at-home orders[15]. In *South-East Asia*, in several countries, military forces have also played a

[8] Ankit Panda, "Indian Army Prepares to Assist in Virus Response Measures", in *The Diplomat*, March 31, 2020, URL: https://thediplomat.com/2020/03/indian-army-prepares-to-assist-in-virus-response-measures/, accessed on August 19, 2020.
[9] *Ibidem.*
[10] Gidget Fuentes, "Beyond Mercy: Navy's COVID-19 Hospital Ship Missions and the Future of Medicine at Sea", *USNI News*, May 25, 2020, URL: https://news.usni.org/2020/05/25/beyond-mercy-navys-covid-19-hospital-ship-missions-and-the-future-of-medicine-at-sea, accessed on August 14, 2020.
[11] Phil Mercer, "Australia Sends In Military to Help Curb COVID-19 Surge", *VOA News*, June 25, 2020, URL: https://www.voanews.com/covid-19-pandemic/australia-sends-military-help-curb-covid-19-surge, accessed on August 30, 2020.
[12] *Ibidem.*
[13] *Ibidem.*
[14] ***, "Two more military medical and nursing teams of the Pacific fleet are sent to help civilian specialists in Kamchatka in the treatment of patients with coronavirus", *Ministry of Defence of the Russian Federation News*, June 18, 2020, URL: https://eng.mil.ru/en/news_page/country/more.htm?id=12297819@egNews, accessed on August 28, 2020.
[15] Adam Isacson, "In Latin America, COVID-19 Risks Permanently Disturbing Civil-Military Relations", on the webpage of *WOLA: Advocacy of Human Rights in the Americas*, July 20, 2020, URL: https://www.wola.org/analysis/latin-america-covid-19-civil-military-relations-policing/, accessed on August 29, 2020.

significant role in coping with the pandemic: "countries with a recent history of military intervention in politics, such as Myanmar and Indonesia, have seen the armed forces take on prominent advisory and decision-making roles. Thailand's government, over which the armed forces exert considerable influence, is reported to have largely excluded civilians from a panel responsible for directing responses to the pandemic"[16].

Helping some sectors of national economies, and maintaining, as much as possible, the normal (or at least an acceptable) pace of economic activities: One of the clearly illustrative episodes of such a nature took place in the United States. Here for example, the Defense Logistics Agency (DLA) has offered a lot of help, in several ways, even if with limited resources, to many of the "12,000 companies DLA works with" (9,000 of these being small business)[17]. A text published by *Defense News* in late July listed some of the forms of help offered by the DLA to these civilian economic entities: a larger share than previously planned of the total DLA's spending went directly to small business (40 %, instead of the assigned goal of 32.36%, previously established by the Department of Defense); and "links to Small Business Administration resources were added to the small business page on DLA's website to help small businesses recover from pandemic struggles"[18]. The same text is also stating "the agency also made it easier for small business contractors to buy non-medical personal protective equipment by opening a new COVID-19 Contingency Store on FedMall", and several online events were organized, in order to significantly boost the chances of small businesses to adapt themselves to the new business environment, and to identify and use new business opportunities[19].

Direct involvement in vaccine production: In late June, for example, important international press agencies were reporting "China's military has received the greenlight to use a COVID-19 vaccine candidate developed by its research unit and CanSino Biologics… after clinical trials proved it was safe and showed some efficacy, the company said…", *Reuters* was reporting, also stating "China's Central Military Commission approved the use of the vaccine by the military on June 25 for a period of one year… The vaccine candidate was developed jointly by CanSino and a research institute at the Academy of Military Science (AMS)"[20]. On that occasion, *Reuters* was underlining the *strictly military use* of the vaccine (a truly exceptional situation); the civilian entity involved in producing the vaccine declared "the Ad5-nCoV is currently limited to military use only"[21]. Dealing with the same piece of news, *Fortune* was reporting the Chinese civilian biotech firm and the military research unit jointly making efforts aimed at developing the cure we are speaking about were "basing the experimental COVID-19 vaccine on their previous collaboration on an Ebola vaccine. The Chinese government approved the Ebola vaccine for widespread use in 2017"[22].

---

[16] Euan Graham, "The armed forces and COVID-19", *International Institute for Strategic Studies* (*IISS)*, April 8, 2020, URL: https://www.iiss.org/blogs/analysis/2020/04/easia-armed-forces-and-covid-19, accessed on August 19, 2020.

[17] Beth Reece, "Defense Logistics Agency helps small businesses during Covid-19 response", in *Defense News*, on the official webpage of the U.S. DoD, URL: https://www.defense.gov/Explore/Features/Story/Article/2282514/defense-logistics-agency-helps-small-businesses-during-covid-19-response/, accessed on August 28, 2020.

[18] *Ibidem.*

[19] *Ibidem.*

[20] ***, "CanSino's COVID-19 vaccine candidate approved for military use in China", *Reuters*, June 29, 2020, URL: https://www.reuters.com/article/us-health-coronavirus-china-vaccine/cansinos-covid-19-vaccine-candi date-approved-for-military-use-in-china-idUSKBN2400DZ, accessed on August 25, 2020.

[21] *Ibidem.*

[22] Grady McGregor, "China's military approves coronavirus vaccine for its own use", *Fortune*, June 29, 2020, URL: https://fortune.com/2020/06/29/china-coronavirus-vaccine-military/, accessed on August 27, 2020.

It might be useful to make, here, some brief comments on *possible political risks associated, in the long run, in some countries, with the massive use of military forces in the fight against the pandemic*. At least on some occasions, the truly exceptional nature of the risks and threats directly associated with the ongoing COVID-19 pandemics has led to a significantly increased role of the military institutions, and, sometimes, of military senior officials. In fully operational states, with strong institutions and stable relations between civilian institutions and military structures, such a role is not to be regarded as a major threat in the long run. Most probably, whenever the consequences of the pandemic are going to be diminished (most probably, after a world-wide distribution of really effective vaccines), the role of the military is going to decrease, until reaching the normal (or pre-pandemic) level. *But when we are speaking about weak states, with a quite recent authoritarian background (including significant elements of military dictatorship), the suddenly increased public role of military structures is legitimately generating truly significant worries*. Such a situation is that of *Indonesia*. In early August 2020, for example, *The Diplomat* has published a text directly dealing with the way in which the role of the military is to be evaluated. Confronted with a massive number and sharp increase of the amount of cases (at that moment roughly 1,500 per day; 100,000 confirmed cases, the largest number in South-East Asia, and a country with just "four doctors and 12 hospital beds for every 10,000 people, and only three intensive care beds per 100,000 people"[23]), the Indonesian state had to extensively rely of resilient institutions, able to at least partially augment the efforts of the health system, badly hit by the pandemic. The source we are quoting here from was clearly stating "there is no doubt that the Indonesian military, as well as the police, has had a prominent and wide-reaching role in combatting the coronavirus. The military has been visible from the national level, including figures around President Joko 'Jokowi' Widodo, all the way down to uniformed personnel providing assistance at the village level. Key military figures include the controversial health minister, retired Army General Terawan Agus Putranto, known for attributing Indonesia's low infection rates at the beginning of the pandemic to God, and head of the National Agency for Disaster Prevention (Badan Nasional Penanggulangan Bencana, BNPB), Lieutenant General Doni Monardo, who is also chief of Indonesia's Coronavirus Disease Response Acceleration Task Force". The same source added "as the virus spread, the role of security forces intensified", and in such a context, "the conspicuous role of the Indonesian armed forces has drawn attention from commentators and analysts who have questioned whether the country's response has been overly militarized. Such concerns are raised as part of a broader discussion about democratic decline not just in Indonesia but across Southeast Asia"[24]. The risk of unbalancing the massively important normal relations between civilian and military institutions, in a way clearly detrimental to democracy and rule of law, is significantly present in other regions as well, in the Indo-Pacific area For example, in several countries of *Latin America* (a region with massive access to the Pacific), where "the COVID-19 pandemic is embedding the armed forces more deeply into citizens' daily lives…, this militarization of public security is greatly concerning because it will be difficult to reverse"[25]. The author we are quoting here from is stating "by placing often unaccountable armed forces side-by-side with citizens for indefinite periods, often at the whim of leaders with a weak commitment to democracy, the pandemic may leave behind a region with a civil-military balance tilted heavily toward the generals"[26].

[23] Natalie Sambhi, "Has COVID Re-Militarized Indonesia?", in *The Diplomat*, August 1, 2020, URL: https://thediplomat.com/2020/07/has-covid-re-militarized-indonesia/, accessed on August 25, 2020.
[24] *Ibidem*.
[25] Adam Isacson, *op. cit.*
[26] *Ibidem.*

2. The impact of COVID-19 on the military manpower resources

From the very beginning of the pandemic, COVID-19 cases were identified in military units (including those deployed abroad), practically anywhere in the world. The number of infections grew larger, but, dealing with *quite many* countries in the Indo-Pacific region, we do not have really accurate data concerning this very problem. There is one *notable* exception, anyhow: we know *a lot* about the situation in the *United States*. To offer some examples, in late April, *Military Times* was reporting, for example, "since late March, the services have averaged between 100 and 200 new cases daily among service members. The most recent count, according to DoD's data, shows 3,438 cases, up from 2,986 on Friday", also adding "the infection rate among service members stands at 1,637-per-million as of Monday, compared with the overall U.S. rate of 2,283-per-million. With 22 deaths so far, DoD's death rate is at 0.4 percent versus the overall U.S. rate of 5 percent"[27]. On July 13, *CNN* was reporting "the US military has seen a spike in COVID-19 cases in recent weeks, with the number of confirmed cases in July growing by about 4,000, a jump of about 60%, according to Defense Department statistics"[28]. According to the same source, at that moment there were "10,554 cases of coronavirus in the military, including forces in the US and overseas, according to Pentagon officials" and "there have been 18,016 cases since the Pentagon started keeping track", and the number of cases needing hospitalization was quite low, white the total number of servicemen killed by the virus was also low ("three individuals")[29]. In early August, *Military Times* was reporting, the U.S. military "showed a continued downward trend in the number of new cases, after spikes in June and July that saw more than 4,000 new cases weekly at one point"; on August 7, total number of military personnel infected with COVID-19 was 30,392, and "of those, 510 have been hospitalized and four have died"[30]. And until August 20, 2020, official U.S. sources are stating, the total number of "presumed COVID-19 cases" directly connected to the military power of the United States reached "over 50,000" (the source we are quoting here from is also stating this figure is including "military, military dependents, DOD civilian employees, and DOD contractors"[31].

The almost complete set of figures dealing with the number of COVID-19 cases in all the structures and units of the U.S. military most clearly is an exceptional case of (probably deliberate) institutional transparency. For other armed forces in the Indo-Pacific region we know almost nothing about the real number of cases and their evolution. In *Russia*, for example, on March 30, official sources said "only three members of the Russian Armed Forces" were "infected by the coronavirus"[32]. A few days later, "on April 4, *Interfax* quoted

[27] Meghann Myers, "The military continues to diagnose more than 100 new COVID-19 cases a day", *Military Times*, April 20, 2020, URL: https://www.militarytimes.com/news/your-military/2020/04/20/the-military-continues-to-diagnose-more-than-100-new-covid-19-cases-a-day/, accessed on August 26, 2020.
[28] Barbara Starr, Ryan Browne, "US military sees 60 percent jump in coronavirus cases in first few weeks of July", *CNN*, July 13, 2020, URL: https://edition.cnn.com/2020/07/13/politics/us-military-covid-spike/, accessed on August 27, 2020.
[29] *Ibidem.*
[30] Meghann Myers, "New military coronavirus cases show lowest increase in months", *Military Times*, August 7, 2020, URL: https://www.militarytimes.com/news/your-military/2020/08/07/new-military-coronavirus-cases-show-lowest-increase-in-months/, accessed on August 31, 2020.
[31] *Coronavirus: DoD Response Timeline*, last updated on August 28, 2020, on the official webpage of the U.S. Department of Defense (DoD), URL: https://www.defense.gov/Explore/Spotlight/Coronavirus/DOD-Response-Timeline/, accessed on August 29, 2020.
[32] Jörgen Elfving, "The Impact of COVID-19 on the Russian Armed Forces", in *Eurasia Daily Monitor Volume 17 Issue 54*, on the webpage of *The Jamestown Foundation*, April 21, 2020, URL: https://jamestown.org/program/the-impact-of-covid-19-on-the-russian-armed-forces/, accessed on August 21, 2020.

an official from the Ministry of Defense who stated that there were no infected persons in the Armed Forces at all". But, as we all know, in mid-April, the Russian president has suddenly postponed "his year's May 9 Victory Day parade", and, until the end of April, "no plans for a new date have been released"[33].

In *China*, the situation is *also* almost completely lacking *any* significant amount of institutional transparency. An analysis published in April by the London-based *IISS* stated "according to one report 3000 PLA personnel had been infected by mid-March"[34]. On the other hand, official Chinese sources have systematically denied there are COVID-19 cases in the ranks of PLA. On March 3, in a moment when practically all "militaries around the " were "seeing their soldiers fall victim to the coronavirus", a headline in an official Chinese military publication was stating "China confirms no cases of coronavirus infection in [the] military"[35]

For *India*, we have *some* data, but almost only in the early stages of the pandemic: on April 18, 2020, for example, the *Hindustan Times* was reporting "a total of 25 Indian Navy personnel have tested positive for Covid-19" (emphasizing the fact that, at that very moment, there were "no cases of infection onboard ships and submarines"; on the same occasion, the same newspaper was reporting "the Army has so far reported eight positive virus cases" – two doctors and one nursing assistant included. Very senior Indian military officials were stating "four are responding well to the treatment"[36].

3. The impact of COVID-19 on military activities of all sorts

In the context of the pandemic, *some military activities have been postponed or interrupted, or at least significantly delayed*. In late March, for example, U.S. and Australian military decided to postpone, at least for a while (to put "on hold") the rotational deployment of roughly 2,500 U.S. Marines to Australia, "as a precaution in the face of the rapidly spreading COVID-19 virus"[37]. On other occasions, the pandemic has led not to cancelling activities, but just to some delays (significant, but not necessarily very long ones). See, for example the case of some U.S. military units, which were deployed abroad *in spite* of the pandemic: on June 9, 2020, the DoD was reporting "more than 400 Idaho Air National Guardsmen with the 124th Fighter Wing deployed from Gowen Field, Idaho, to various locations in support of Operations Freedom's Sentinel, Inherent Resolve and New Normal"[38]. The official source we are quoting here from added "although they experienced delays due to global circumstances, the majority of airmen in the deployment package have now left Idaho, followed closely by 254 short tons of cargo"[39].

---

[33] *Ibidem.*
[34] Euan Graham, *op. cit.*
[35] John Xie, "China Claims Zero Infections in Its Military", *VOA News*, April 6, 2020, URL: https://www.voanews.com/science-health/coronavirus-outbreak/china-claims-zero-infections-its-military, accessed on August 25, 2020.
[36] Rahul Singh, "Coronavirus update: 25 Indian Navy personnel test positive for Covid-19", *Hindustan Times*, April 18, 2020, URL: https://www.hindustantimes.com/india-news/covid-19-outbreak-at-least-20-indian-navy-personnel-test-positive-for-coronavirus/story-9zFtU4xynEj3Yf2NqVyCRI.html, accessed on August 29, 2020.
[37] Shawn Snow, "Marine rotation to Australia 'on hold' over COVID-19 concerns", *Marine Corps Times*, March 20, 2020, URL: https://www.marinecorpstimes.com/news/coronavirus/2020/03/21/marine-rotation-to-australia-on-hold-over-covid-19-concerns/, accessed on August 19, 2020.
[38] Taylor Walker (Air Force Airman 1st Class), "Packing resilience: Idaho airmen deploy during COVID-19 pandemic", in *Defense News* (on the official webpage of the Department of Defense), at URL: https://www.defense.gov/Explore/Features/Story/Article/2211518/packing-resilience-idaho-airmen-deploy-during-covid-19-pandemic/, text accessed on August 22, 2020.
[39] *Ibidem.*

On some occasions we know *a lot* about, *COVID-19 has already generated significantly increased tensions on the international arena, including harming, a lot, some solid relations between important and stable strategic partners and allies*. See, for example, the case of U.S.-Japan relations in the context of the sharp increase of the total number of COVID-19 cases among the U.S. troops deployed to Okinawa. In July, *Deutsche Welle (DW)* was reporting, 98 cases were reported in American military bases in Okinava – the "US Marine Corps Air Station Futenma… and nearby Camp Hansen", and some "isolated cases have also been reported at Kadena Air Base, Camp McTureous and Camp Kinser[40]. The number was not necessarily very high, but the percentage was. The total number of U.S. troops deployed to Okinawa was "26,000", and the total number of *local* cases in the prefecture (which has a population of roughly 1.5 million people) was only 148. In such a situation, Okinawa Governor Denny Tamaki went directly to Tokyo, in order "to call on the US ambassador and representatives of the Japanese government to halt the transfer of any more US military personnel to the prefecture"[41]. Japanese official sources reported the Okinawa governor also wanted to be swiftly discussed and implemented some more sensitive *political* measures, including "a comprehensive review of the Status of Forces Agreement between the two nations"[42].

We also know that, on some occasions, *the pandemic has been regarded by some states as an important window of opportunity at geo-strategic level*. Some authors are directly stating, for example, at least some of the actions of all sorts of the Chinese armed forces (officially called the People's Liberation Army) "may have been carried out to exert some pressure on and even probe the responses and resilience of the US, Taiwanese and other regional militaries"[43]. We might place such an evaluation in direct connection with authors and texts evaluating the way is which China's military managed to face the pandemic shock: in early May 2020, for example, a study published by the global think tank *International Institute for Strategic Studies (IISS)* was openly stating "the COVID-19 outbreak will continue to prove a test for the JLSF[44], the creation of which was intended as a major part of the reform of the PLA's command and logistics system". The author of the study (Meia Nouwens, Research Fellow for Chinese Defence Policy and Military Modernisation) was also stating, at that very moment, "although the pandemic has impacted some military training and exercises, as well as China's sprawling defence-manufacturing and research-and-development base, the PLA is likely to escape lasting damage"[45].

Some final remarks and brief conclusions

Most obviously, any serious study of the multi-faceted impact of the COVID-19 pandemic on the military has to seriously take into consideration the problem of *resilience*. In mainly military terms, resilience is defined by the U.S. DoD as being "as the ability to

[40] Julian Ryall, "Okinawa shocked at cluster of coronavirus cases on US military bases", *Deutsche Welle (DW)*, July 14, 2020, URL: https://www.dw.com/en/okinawa-shocked-at-cluster-of-coronavirus-cases-on-us-military-bases/a-54168481, accessed on August 30, 2020.
[41] *Ibidem.*
[42] *Ibidem.*
[43] Meia Nouwens, *op. cit.*
[44] A.N.: JLSF is the Joint Logistics Support Force of the Chinese armed forces (People's Liberation Army - PLA), a structure established in 2016.
[45] Meia Nouwens, *op. cit.*

withstand, recover, and grow in the face of stressors and changing demands"[46]. Resilience is the segment of reality allowing individuals (but also *collective* actors, including institutions) "to adapt well in the face of adversity, trauma, tragedy, threats, or significant sources of stress"[47]. Another text, published in 2018 by a quite large collective of authors, some of them belonging to research institutions directly involved in military activities and / or institutional structures (see for example: Army Personnel Research Capability, HQ, Army, UK; Norwegian Defense Research Establishment, FFI, Norway; CFWMS Human Performance and Development Canadian Armed Forces, Canada; and U.S. Army Research Institute of Environmental Medicine, United States), is stating modern military operations of all sorts, including combat and other warfare activities, "often occur in volatile, uncertain, complex, and ambiguous (VUCA) environments accompanied by physical exertion, cognitive overload, sleep restriction and caloric deprivation. The increasingly fast-paced nature of these operations requires military personnel to demonstrate readiness and resiliency in the face of stressful environments to maintain optimal cognitive and physical performance necessary for success"[48]. The same text is defining *resilience* as being "the capacity to overcome the negative effects of setbacks and associated stress on performance" [49].

As far as we can understand, military forces usually are (almost anytime and anywhere) significantly more resilient than the rest of institutions, than local, regional, and national communities, than the average individual. It is quite easy to understand such a reality: it is a matter of selection of manpower, a matter of training, a matter of effectiveness of military logistics, a matter of strict discipline, a matter of effective materiel. It is too early to conclude, at this very moment, *if* the military resilience managed to properly consolidate general resilience of societies / nations in the context of the COVID-19 pandemic. But, most obviously, *after* the end of the pandemic researchers of all sorts might have a serios incentive to explore ways of enhancing the general level of resilience of states, institutions, communities (from tiny ones to nations).

Another topic for some future research might be connected to *the impact of the pandemic on the stability of the international system*. It is also too early to reach definitive conclusions, but we might take into account a direct warning dealing with the geo-strategic consequences of COVID-19: in early June, the acting director of the *Atlantic Council's Scowcroft Center* has published a text in which he said "the increased probability of a U.S.-China military confrontation is one… potential secondary shock" directly generated by the ongoing pandemic; more than this, he openly stated, "the chances of conflict in the coronavirus era are higher than before the pandemic"[50].

---

[46] Joachim Roski, Bruce L. Gillingham, Jeffrey Millegan, et al., "Building Resilience For Greater Health And Performance: Learning From The Military", on the *Health Affairs* webpage, August 12, 2019, URL: https://www.healthaffairs.org/do/10.1377/hblog20190807.768196/full/, accessed on August 25, 2020.
[47] *Ibidem.*
[48] Bradley C. Nindl, Daniel C. Billing, Jace R. Drain, et al., "Perspectives on resilience for military readiness and preparedness: Report of an international military physiology roundtable", in *Journal of Science and Medicine in Sport*, Vol. 21, Issue 11, November 2018, pp. 1116-1124, URL: https://www.sciencedirect.com/science/article/pii/S1440244018301397, accessed on August 29, 2020.
[49] *Ibidem.*
[50] Barry Pavel, "The Coronavirus Is Raising the Likelihood of Great-Power Conflict", in *Defense One*, June 1, 2020, URL: https://www.defenseone.com/ideas/2020/06/coronavirus-raising-likelihood-great-power-conflict/165798/, accessed on August 27, 2020.

BIBLIOGRAPHY:

1. ***, "CanSino's COVID-19 vaccine candidate approved for military use in China", *Reuters*, June 29, 2020, URL: https://www.reuters.com/article/us-health-coronavirus-china-vaccine/cansinos-covid-19-vaccine-candidate-approved-for-military-use-in-china-idUSKBN2400DZ
2. ***, "Two more military medical and nursing teams of the Pacific fleet are sent to help civilian specialists in Kamchatka in the treatment of patients with coronavirus", *Ministry of Defence of the Russian Federation News*, June 18, 2020, URL: https://eng.mil.ru/en/news_page/country/more.htm?id=12297819@egNews
3. BREWSTER, Murray, "Canadian military intelligence unit issued warning about Wuhan outbreak back in January", *Canadian Broadcasting Corporation* (*CBC)*, April 10, 2020, URL: https://www.cbc.ca/news/politics/coronavirus-pandemic-covid-canadian-military-intelligence-wuhan-1.5528381
4. BRZEZINSKI, Zbigniew, *Marea tablă de șah: Supremația americană și imperativele sale geostrategice*, Univers Enciclopedic, Bucharest, 2000.
5. *Coronavirus: DoD Response Timeline*, last updated on August 28, 2020, on the official webpage of the U.S. Department of Defense (DoD), URL: https://www.defense.gov/Explore/Spotlight/ Coronavirus/DOD-Response-Timeline/
6. ELFVING, Jörgen , "The Impact of COVID-19 on the Russian Armed Forces", in *Eurasia Daily Monitor Volume 17 Issue 54*, on the webpage of *The Jamestown Foundation*, April 21, 2020, URL: https://jamestown.org/program/the-impact-of-covid-19-on-the-russian-armed-forces/
7. FUENTES, Gidget, "Beyond Mercy: Navy's COVID-19 Hospital Ship Missions and the Future of Medicine at Sea", *USNI News*, May 25, 2020, URL: https://news.usni.org/2020/05/25/beyond-mercy-navys-covid-19-hospital-ship-missions-and-the-future-of-medicine-at-sea
8. GRAHAM, Euan, "The armed forces and COVID-19", *International Institute for Strategic Studies* (*IISS)*, April 8, 2020, URL: https://www.iiss.org/blogs/analysis/2020/04/easia-armed-forces-and-covid-19
9. MCGREGOR, Grady, "China's military approves coronavirus vaccine for its own use", *Fortune*, June 29, 2020, URL: https://fortune.com/2020/06/29/china-coronavirus-vaccine-military/
10. Mercer, Phil, "Australia Sends In Military to Help Curb COVID-19 Surge", *VOA News*, June 25, 2020, URL: https://www.voanews.com/covid-19-pandemic/australia-sends-military-help-curb-covid-19-surge
11. MYERS, Meghann, "New military coronavirus cases show lowest increase in months", *Military Times*, August 7, 2020, URL: https://www.militarytimes.com/news/your-military/2020/08/07/new-military-coronavirus-cases-show-lowest-increase-in-months/
12. MYERS, Meghann, "The military continues to diagnose more than 100 new COVID-19 cases a day", *Military Times*, April 20, 2020, URL: https://www.militarytimes.com/news/your-military/2020/04/20/the-military-continues-to-diagnose-more-than-100-new-covid-19-cases-a-day/
13. NAISBITT, John; ABURDENE, Patricia, *Anul 2000 – Megatendințe: Zece noi direcții pentru anii '90*, Humanitas, Bucharest, 1993.
14. NINDL, Bradley C.; BILLING, Daniel C.; DRAIN, Jace R. et al., "Perspectives on resilience for military readiness and preparedness: Report of an international military physiology roundtable", in *Journal of Science and Medicine in Sport*, Volume 21, Issue 11, November 2018, URL: https://www.sciencedirect.com/science/article/pii/S1440244018301397
15. NOUWENS, Meia, (Research Fellow for Chinese Defence Policy and Military Modernisation), *China's armed forces and the impact of COVID-19*, on the webpage of the International Institute for Strategic Studies (IISS), URL: https://www.iiss.org/blogs/military-balance/2020/05/china-armed-forces-covid-19-pla

16. PANDA, Ankit, "Indian Army Prepares to Assist in Virus Response Measures", in *The Diplomat*, March 31, 2020, URL: https://thediplomat.com/2020/03/indian-army-prepares-to-assist-in-virus-response-measures/
17. PAVEL, Barry, "The Coronavirus Is Raising the Likelihood of Great-Power Conflict", on *Defense One* webpage, June 1, 2020, URL: https://www.defenseone.com/ideas/2020/06/coronavirus-raising-likelihood-great-power-conflict/165798/
18. REECE, Beth, "Defense Logistics Agency helps small businesses during Covid-19 response", in *Defense News*, on the official webpage of the U.S. DoD, URL: https://www.defense.gov/Explore/Features/Story/Article/2282514/defense-logistics-agency-helps-small-businesses-during-covid-19-response/
19. ROSKI, Joachim; GILLINGHAM, Bruce L.; MILLEGAN, Jeffrey et al., "Building Resilience For Greater Health And Performance: Learning From The Military", on the Health Affairs webpage, August 12, 2019, URL: https://www.healthaffairs.org/do/10.1377/hblog20190807.768196/full/
20. RYALL, Julian, "Okinawa shocked at cluster of coronavirus cases on US military bases", *Deutsche Welle (DW)*, July 14, 2020, URL: https://www.dw.com/en/okinawa-shocked-at-cluster-of-coronavirus-cases-on-us-military-bases/a-54168481
21. SAMBHI, Natalie, "Has COVID Re-Militarized Indonesia?", in *The Diplomat*, August 1, 2020, URL: https://thediplomat.com/2020/07/has-covid-re-militarized-indonesia/
22. SINGH, Rahul, "Coronavirus update: 25 Indian Navy personnel test positive for Covid-19", *Hindustan Times*, April 18, 2020, at URL: https://www.hindustantimes.com/india-news/covid-19-outbreak-at-least-20-indian-navy-personnel-test-positive-for-coronavirus/story-9zFtU4xynEj3Yf2NqVyCRI.html
23. SNOW, Shawn, "Marine rotation to Australia 'on hold' over COVID-19 concerns", *Marine Corps Times*, March 20, 2020, URL: https://www.marinecorpstimes.com/news/coronavirus/2020/03/21/ marine-rotation-to-australia-on-hold-over-covid-19-concerns/
24. STARR, Barbara; BROWNE, Ryan, "US military sees 60 percent jump in coronavirus cases in first few weeks of July", *CNN*, July 13, 2020, URL: https://edition.cnn.com/2020/07/13/politics/us-military-covid-spike/
25. WALKER, Taylor, Air Force Airman 1st Class, "Packing resilience: Idaho airmen deploy during COVID-19 pandemic", in *Defense News* (on the official webpage of the Department of Defense), URL: https://www.defense.gov/Explore/Features/Story/Article/2211518/packing-resilience-idaho-airmen-deploy-during-covid-19-pandemic/
26. WIGHT, Martin, *Politica de Putere*, Ed. Arc, Chișinău, 1998 (original title: *Power Politics*, Pinter Publisher Ltd., 1997).
27. XIE, John, "China Claims Zero Infections in Its Military", *VOA News*, April 6, 2020, URL: https://www.voanews.com/science-health/coronavirus-outbreak/china-claims-zero-infections-its-military

FIGHTING POLYCEPHALIC THREATS – THE SECURITY ENVIRONMENT IN TIMES OF PANDEMICS AND INFODEMICS

George-Sorin MARIN
Master's student, "Crises management" Programme,
Faculty of Business and Administration, University of Bucharest, Romania.
E-mail: marin_sorin15@yahoo.com

Abstract: *The expression "the world is facing a crisis" almost became a cliché these days. During the global response to fight the COVID-19 crisis, a developing kind of threat gained new valences and the capacity to spread almost instantly, due to the characteristics of the Information Age we live in. The over-abundance of information generated a new challenge for humanity and affected the process of finding reliable, trustworthy sources of information during the pandemic. Propaganda, false narratives and disinformation inhibit governmental processes aimed to overcome the crisis. Strategic decisions have to take into consideration multiple risks and factors in order to prevent both infections and infoxications. Therefore, the security environment has the complex mission to manage a sanitary crisis that endangers the health of populations all over the world in a new type of confrontation – a campaign against polychephalic threats.*

Keywords: *crisis; pandemic; infodemic; communication; fake news; disinformation; misinformation.*

Introduction

What happens to the security environment's dynamic when the chief of the World Health Organization (WHO) publicly declares that the world we live in is not just fighting an epidemic, but also an infodemic[1]? Does it mean that the governments and national authorities have to confront two types of threats simultaneously? How do they prioritize the enemies – is the new virus, the enemy of citizens' health, the first one to eradicate or is the infodemic conceived around it, the enemy of social reasoning and judgement, the most dangerous threat? How can both crises be managed at the same time and why are they so interconnected?

This paper aims to present a series of elements that can amplify the knowledge needed in order to generate a comprehensive answer to the questions raised above, focusing on two dimensions of the *Novel Coronavirus* crisis and its multiple implications on several plans: security, public health, society and the decision-making process.

1. Conceptualization of pandemics and infodemics

It is essential to clearly understand the meaning of the main terms this paper is built around. According to WHO, a pandemic is the "worldwide spread of a new disease"[2]; the

[1] ***, "UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis", *United Nations*, 2020, URL: https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19, accessed on 28.04.2020.
[2] ***, "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020", *World Health Organization*, 2020, URL: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, accessed on 30.04.2020.

COVID-19 outbreak has been labelled as a pandemic on March 11th, 2020, becoming the first one caused by a Coronavirus.

As information of the virus deluges traditionally and on social media, WHO also explains indofemics, referring to them as "excessive amounts of information about a problem, which makes it difficult to identify a solution". Also known as "infobesity" or "infoxication", the term describes the difficulty of understanding an issue and effectively making decisions when one has too much information about that concern[3].

Even though the two words are from different domains, one being a medical term and the other one referring to our modern information space, there is a list of similarities between them. Firstly, both of them are characterized by high spreading rates; however, according to WHO's director-general, the infodemic "spreads faster and more easily than the virus"[4]. Secondly, their constitutent elements signal a significant threat to people's safety and security. While an infection with the *Novel Coronavirus* can ultimately lead to fatality, the infodemic consisting in fake news spreading, misinformation and disinformation can potentiate this effect. The infodemic has worsened the global health crisis and revealed a series of deficiencies associated with problems of communication and organization.

Furthermore, a distinction between the component terms of the infodemic phenomenon is crucial for the content of the current research. *Misinformation* is defined in several ways, but a relevant description for the purpose of this paper consists of "falsehoods and rumors propagated without a broad political aim, either with or without malicious intent that achieves viral status"[5]. On the other hand, *disinformation* represents "false information spread deliberately to deceive people"[6], while propaganda, although it has many official definitions with subtle nuances, mainly refers to "the deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behavior to achieve a response that furthers the desired intent of the propagandist"[7]. Last but not least, *fake news* is "the deliberate presentation of false and misleading claims as news with a deliberate design to mislead"[8].

The two terms – *pandemic* and *infodemic* – put together accurately describe the biggest crisis our generation has to face, a case that could be classified as a *polychephalic threat*. The word originates from the Greek stems *poly* (meaning "many") and *kephalē* (meaning "head") and it has mythological references, basis for the following part of this paper, a metaphorical comparison between the ancient stories and the crises of the year 2020.

2. Mythology today – the two-headed threat

In the Greek mythology, Orthrus (the brother of Cerberus) was a monstrous hound, a two-headed dog who guarded Geryon's cattle and was encountered and killed by the

[3] Yang, Christopher C.; Chen, Hsinchun and Hong, Kay, *Visualization of large category map for Internet browsing*, in *Decision Support Systems*, vol. 35, Issue 1, Elsevier, 2003, pp. 89-91.
[4] *Munich Security Conference*, World Health Organization, 2020, URL: https://www.who.int/dg/speeches/detail/munich-security-conference, accessed on 02.05.2020.
[5] *Policy Report – Fake News: National Security in The Post-Truth Era*, RSIS – S. Rajaratnam School of International Studies, 2018, URL: http://journres1.pbworks.com/w/file/fetch/135129183/Fake_News_National_Security_in_the_Post-.pdf, accessed on 04.05.2020.
[6] Pacepa, Ion Mihai and Rychlach, Ronald J., *Dezinformarea*, Humanitas, Bucharest, 2015, p. 5.
[7] Jowett, Garth S. and O'Donnell, Victoria, *Propaganda & Persuasion – Fifth Edition*, SAGE Publications, Thousand Oaks, 2012, p. 7.
[8] Gelfert, Axel, *Fake News: A Definition*, in *Informal Logic*, vol. 38, no. 1, pp. 84-85, URL: https://informallogic.ca/index.php/informal_logic/article/view/5068, accessed on 09.05.2020.

Heracles[9]. Even though mythology consists of legends and stories, during this research I found a potential analogy between myths and the current threats to the security environment.

Therefore, in the elaboration process of this paper I found the relationship between mythology and security environment to be accurate, due to the security implications a single and unique problem can develop. How can two-headed dog from Greek mythology be transposed to a 2020's global security problem? The nature and the structure of threats haven't withdrawn, they have just been modified. Alongside humanity, risks and threats evolved, but their catalyzing factor is almost the same. If the mythological two-headed dog's mission was to hold back physical access to the cattle, the current infodemic jeopardizes the access to relevant, reliable information.

In a mythological Era, the specific problem could be solved directly/physically, but the crisis nowadays is about knowledge, trust and support. One thing that makes this pandemic different than its predecessors is the dominance and the influence of social media in today's world; in the current times, social media is both a blessing and a curse during the pandemic. Social media platforms may represent a dangerous and vulnerable socio-technical solution in times of crisis.

During times of disaster or emergency, urgent problems arise and require immediate response. When complex emergencies occur, public officials are cautious about making pronouncements that can be premature, instead of carefully craft statements to ensure accuracy and avoid disinformation/misinterpretation. In the digital age, the constant need of analyzing, assessing and communicating information has to compete with the instantaneous spreading of misinformation on the Internet and social media platforms. Also, misinformation can be found in many forms, from rumours to conspiracy theories or exaggerated/untrue medical claims and hoaxes.

The impact of misinformation may be even more pronounced, because of the so-called confirmation bias, which refers to the seeking or interpreting of evidence in ways that are partial to existing beliefs, expectations or a hypothesis in hand[10]. Internet content may reinforce society's pre-existing biases and prejudices, fueling a non-productive behavior to combat the health crisis. Social media facilitates a prejudiced collective behavior organizing similar to crowdsourcing, which rapidly enlists a large number of people. The frequency of situations like this will most likely increase, given the ways in which human connection is able to intensify.

When it comes to health, misinformation's consequences can be disastrous. Making people fearful and leading them to take fewer measures to protect themselves and prevent the transmission of the disease, the infodemic hampers society's health and the strategic response to the pandemic. Misinformation frequently evokes a strong emotional cocktail – surprise, fear, anxiety, anger or anything that motivates people into sharing the "information" with others. Assistant Professor Dustin Carnahan, Ph.D., from the Department of Communication of the Michigan State University, noticed similarities between the way people consume information in the political sphere and their reactions to the Coronavirus news[11]. An individual's reaction may come down to the values and beliefs that inform their own ideology.

---

[9] *Chapter Four: Metamorphosis*, The Department of Classics of the Ohio State University, n. d., URL: https://classics.osu.edu/sites/classics.osu.edu/files/Johnston_Metamorphosis_Chapter_for_sharing_August_27_2015[1].pdf, accessed on 12.05.2020.

[10] Nickerson, Raymond S., *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, in *Review of General Psychology*, vol. 2, no. 2, Education Publishing Foundation, 1998, pp. 175-176.

[11] *The COVID-19 Infodemic: Combatting 'Dangerous' Misinformation on Social Media*, The Department of Communication of the Michigan State University, 2020, URL: https://comartsci.msu.edu/about/newsroom/news/covid-19-infodemic-combatting-dangerous-misinformation-social-media, accessed on 16.05.2020.

The way of dealing with this *polychepalic threat* must be meticulously analyzed; towards supporting this assertion, a simple analogy might prove to be relevant. In order to stop the pandemic, governments take measures in order to make citizens stay safe, at home. Indoors, due to the direct and digital access to information, they are at risk. This time, the risk is not health-related, it is an informational risk generated by fake news and complementary phenomena. Orthrus is back and he is stronger, more dangerous and more resilient. It is the mission of international organizations, governments, healthcare agencies, social media platforms and individuals to put their efforts together in a coordinated and strategic manner in order to defeat the *polychepalic threat*.

3. A new war of influence. The disinformation threat landscape

The usage of the COVID-19 pandemic as an information weapon is both an element of the external, but also of the internal political struggle among the global security environment.

In a study[12] realized by UNESCO, nine key themes of the COVID-19 disinformation were identified: *a)* the origins and spread of the coronavirus; *b)* false and misleading statistics; *c)* economic impacts; *d)* discrediting of journalists and credible news outlets; *e)* medical science (symptoms, diagnosis and treatment); *f)* impacts on society and the environment; *g)* politicization; *h)* content driven by fraudulent financial gain; *i)* celebrity-focused disinformation.

World's best collective efforts to curtail Coronavirus' effects are clearly obstructed by the impressive amount of information on the subject. Europol's study[13] on the subject reveals that the spreading misinformation can start from various sources and, implicitly, their objectives can differ. For example, individuals/criminals can seek profit and states/state-backed actors might try to identify ways to advance their geopolitical interests. Moreover, there is an increase of opportunists looking to discredit official sources. Disinformation and misinformation may have serious effects and repercussions in this case, including the jeopardizing of public health and endangering people's lives.

The range of potential victims gets even larger, due to the fact that a massive number of people are teleworking from home, often with outdated security systems. Therefore, cybercriminals might seize the opportunity and take advantage of the situation and increase their activities' extent. Europol highlights the fact that cybercriminals have been among the most adept at exploiting the COVID-19 pandemic for the various scams and attacks[14]; the study suggests that active criminals in the domain of cybercrime have been able to adapt quickly and capitalize on the fears/anxieties of their victims.

The facts above can signify that life under lockdown is not only changing how people live, but also how crime occurs. COVID-19 has provided an opportunity for malign actors to exploit the informational space for harmful purposes.

Also, the pandemic crisis showed the world how powerful are a series of state actors' propaganda machines. China confronted a significant challenge because of the Information War, due to the outbreak of the *Novel Coronavirus*. When COVID-19 was called a "Chinese virus" by the United States' president, Donald Trump, official Chinese accounts adopted a

[12] *DISINFODEMIC: Deciphering COVID-19 disinformation*, UNESCO, 2020, URL: https://en.unesco.org/covid19/disinfodemic/brief1, accessed on 22.05.2020.
[13] *COVID-19: FAKE NEWS*, Europol, 2020, URL: https://www.europol.europa.eu/covid-19/covid-19-fake-news, accessed on 23.05.2020.
[14] *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, Europol, 2020, URL: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, accessed on 24.04.2020.

confrontational posture in their messaging on the virus (in late February and throughout March 2020). Both China and Russia amplified conspiracy theories, disinformation campaigns, seeking to sow doubt about the Western countries' handling of the crisis. With the usage of social media, discredited and sometimes contradictory theories dispersed, Occidental states' measures to manage the countries were undermined.

Denis MacShane, a former UK Minister of State for Europe, proposed a "renaming" of the virus as the "conspiracy virus" or "fake news 19"[15], as the Chinese and Russian governments have used the pandemic to spread disinformation, especially across social media.

Furthermore, the Chinese propaganda machine was used as a tool to turn the tables in the communist regime's interest and shape the narrative of the crisis. The Chinese authorities launched a vast operation involving sending medical equipment (masks, gloves, ventilators, diagnostic tests) and experts to the affected European states. According to specialists of the Atlantic Council, "there is clear good in such actions, but one cannot ignore China's other geopolitical objectives in play"[16]. The Chinese government promoted news of the medical supplies sent to other countries without mentioning that only a small share are donations. Basically, China over-magnified its assistance using public diplomacy and social media, starting a serious war of influence and an active information campaign with visible results. For example, in April, a poll revealed that 52% of Italy's citizens viewed China as a friendly country, while Germany and France were considered "enemies"[17].

While the effectiveness of disinformation as a policy tool used by some state actors remains unclear, information warfare is a serious and growing threat since there are real victims of manipulations of opinion processes and false narratives. Understanding the challenges posed by the *polychephalic threat* is vital for the future of democracies, especially since Europe and the West are probable to be targets of disinformation and influence operations. The European Union should consider its actions from the perspective of denying hostile actors the benefits of their actions[18] in order to reshape adversaries' strategic calculus.

4. Forging cooperation for crisis response. The art of crisis communication

As increasingly complex threats require complex solutions, pandemics and infodemics require coordinated global response strategies. However, the strategies need to have a multidomain characteristics/structures, requiring medical knowledge and expertise that have been proved efficient against the new Coronavirus and socio-political, cultural and psychological approaches. Moreover, social media networks and digital corporations are vital in order to develop a successful strategy of this kind. They represent the place where misinformation thrives and they must use the same tools to fight against the infodemic. It is clear that, in order to overcome the crisis, comprehensive approaches are needed, involving multiple actors from governments, militaries, the private sector and civil society.

A potential solution might consist in social media companies to sort, rank and prioritize reliable information, especially during crises. Concrete similar examples have been materialized – for example, on the 18th of March 2020, Facebook, the world's largest social

[15] Dempsey, Judy, *Judy Asks: Is the Coronavirus Breeding Disinformation Across Europe?*, 2020, URL: https://carnegieeurope.eu/strategiceurope/81508, accessed on 26.05.2020.
[16] *Is China winning the coronavirus response narrative in the EU?*, The Atlantic Council, 2020, URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/is-china-winning-the-coronavirus-response-narrative-in-the-eu/, accessed on 28.05.2020.
[17] Zeneli, Valbona and Santoro, Federica, *China's Disinformation Campaign in Italy*, 2020, URL: https://thediplomat.com/2020/06/chinas-disinformation-campaign-in-italy/, accessed on 28.05.2020.
[18] Pamment, James, *The EU's Role in Fighting Disinformation: Taking Back the Initiative*, 2020, URL: https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286, accessed on 17.07.2020.

media platform, launched the "Coronavirus Information Center"[19], an initiative aiming to help people find relevant information and tips. Also, when users search "coronavirus" on the platform, Facebook shows a banner that directs them to the WHO official site or national health organizations. All social networks should continue to sponsor official information sources and correct or eliminate the false claims about the pandemic.

However, such efforts have to be integrated with governmental institutions' measures and national/international healthcare agencies' directions in order to develop an effective strategy to combat the referential *polychephalic threat*. The biggest part of the year 2020 represented and invaluable test for crisis communication and a real learning platform. It has become a necessity for all countries to coordinate together in order to counter the new levels of disinformation and propaganda. Governments can lead by example and negotiate with social media and big tech companies in order to promote reliable guidance and public health information. After all, *the best antidote to bad information is good information*.

In a nutshell, cooperation between different sectors is needed – social media platforms should increase their efforts to prevent disinformation from spreading online, while governments and international organizations have to find solutions to the critical needs of these moments. The best defense is a collective one – a successful response to the COVID-19 crisis requires a coordinated multi-stakeholder effort to combat the disinformation around it, with clear public leadership.

In order to mitigate the *polychephalic threats*, governments have to stand with their people and to build a trusted relationship. People expect their leaders to be present in their world. The spread of the fake news about coronavirus showcase humans' real need to feel included. Research shows that individuals are drawn to conspiracy theories when they feel powerless or anxious[20], since they give humans a sense of control over a situation they might not understand. Rather than pointing the finger at their citizens for spreading misinformation or conspiracy theories, governments should make efforts to help them access the right information via the right channels.

The ways citizens act to disinformation is a reflection of how successfully authorities, in cooperation with communities, are capable of establishing security in society. The countries with a higher level of trust (regardless of political regime) have been more successful in combating the pandemic than those with lower trust levels[21]. In times of crisis, effective communication is crucial, especially when social media is swirling with misinformation. Strategic and transparent communication should be among the first lines of action for public institutions at all levels[22].

Crisis communication highlights legitimation strategies, but also indicates how government institutions themselves make sense of crises[23]. An analysis[24] realized by experts

---

[19] Holmes, Aaron, *Facebook is launching a new 'coronavirus information center' that will appear at the top of people's News Feeds*, 2020, URL: https://www.businessinsider.com/facebook-coronavirus-information-center-news-feed-feature-covid-2020-3, accessed on 03.06.2020.

[20] Grzesiak-Feldman, Monika, *The Effect of High-Anxiety Situations on Conspiracy Thinking*, in *Current psychology*, vol. 32, Springer Publishing, 2013.

[21] Gunhild Hoogensen, Gjørv, *Coronavirus, invisible threats and preparing for resilience*, 2020, URL: https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html, accessed on 14.06.2020.

[22] *Transparency, communication and trust: The role of public communication in responding to the wave of disinformation about the new Coronavirus*, Organisation for Economic Co-operation and Development, 2020, URL: https://www.oecd.org/coronavirus/policy-responses/transparency-communication-and-trust-bef7ad6e/#back-endnotea0z3, accessed on 19.07.2020.

[23] Brandt, Philipp and Wörlein, Jan, *Government crisis communication during the coronavirus crisis: Comparing France, Germany, and the United Kingdom*, 2020, URL: http://www.cso.edu/fiche_actu.asp?actu_id=2570, accessed on 22.07.2020.

[24] *COVID-19: Crisis Communications*, Tony Blair Institute for Global Change, 2020, URL: https://institute.global/sites/default/files/inline-files/Crisis%20Communications.pdf, accessed on 23.07.2020.

of the Tony Blair Institute for Global Change classified some key strategic levers that governments should target in these critical moments:

a) *suppress* – the coordination of a response across governments that emphasizes saving lives; enforcing a behavior change in order to suppress the outbreak by remaining in isolation and practicing social distancing;

b) *test and trace* – the process of eliminating the testing fears citizens back; transparency about the real availability of testing solutions;

c) *revive* – the coordination of national economic response plan; inducing the message that government is doing everything it can to stabilize markets, protect livelihoods, and return to economic growth.

Despite the utility of the analysis in the decision-making process, an optimized crisis communication carried out by national leaders and authorities should also focus on "the other head" of the crisis, the threat caused by the infodemic. This type of approach would have a dual advantage – supporting the effective implementation of emergency measures and satisfying the need for accurate and definitive information. The crisis leader needs to discharge two roles: engaging in authentic human acts and delivering institutional messages[25]. In a larger perspective, the leaders need to offer their people an *open response*, one of the main recommendations of the specialists of the Open Government Partnership. According to them, "open response measures place transparency, accountability, and participation at the center of immediate government efforts to curb contagion and provide emergency assistance"[26]. In terms of processes and institutions that are necessary to be involved in achieving the open response goal, the fundamental ones consist of a multi-stakeholder advisory council, support for the civil society organizations whose funding is at risk as a result of the crisis, workplace protections and a very important component – the digital civic space[27].

While one of the biggest issues governments face is to maintain clear and direct communication with their citizens and, implicitly, the open response component, the technologization and the rise of the digital age can outline the optimal solution to this issue. The tools that can be used to address this problem and employ a better and proactive communication consist of different digital and online solutions that the majority of the citizens can access. Communication experts communicators, health professionals, and international organisations have advocated using social media to engage audiences beyond mass information dissemination. To combat fake news, it is important for authorities to use the same channels that disseminate and feed it. Social media facilitates a more conversational, dialogic approach, allowing leaders to present a "human face" to the crisis[28]. Therefore, constructive engagement with citizens on social media provides leaders an opportunity during times of crisis to explain their decision-making and to transmit key messages to their audience.

The communicative act of sharing emotional and empathetic messages on various channels and the usage of a language that places the leader on the same level as his followers, while still performing courage and confidence in a context dominated by uncertainty have the potential to frame the major crisis event as something normal and solvable. Transparency,

[25] Gigliotti, Ralph A., *Leader as Performer; Leader as Human: A Discursive and Retrospective Construction of Crisis Leadership*, in *Atlantic Journal of Communication*, vol. 24, no. 4, Taylor and Francis, 2016, pp. 185-188.
[26] *A Guide to Open Government and the Coronavirus: Open Response + Open Recovery*, Open Government Partnership, 2020, p. 5, URL: https://www.opengovpartnership.org/wp-content/uploads/2020/06/OGP-Guide-to-Open-Gov-and-Coronavirus.pdf, accessed on 26.08.2020.
[27] *Ibidem*.
[28] Kulkarni, Vaibhavi, *Is It the Message or the Medium? Relational Management during Crisis through Blogs, Facebook and Corporate Websites*, in *Global Business Review*, vol. 20, no. 3, SAGE Publications, Thousand Oaks, 2019, pp. 743-756.

diplomacy and collaboration might be the best tools that any government can use, preeminently since "everything is communication, especially in a crisis"[29].

Conclusions

The current issue is much bigger than COVID-19; it's a reminder about the major problem of fake news, misinformation and disinformation – phenomena that are challenging to fight even in normal circumstances. The ongoing Coronavirus crisis is creating a favorable climate for disinformation and fake news spreading and, implicitly, opportunities for the adversarial actors of the European Union to exploit.

Generally, crises lead to insecurity and uncertainty – citizens are confused and governments have to take important decisions and settle on specific policies. Applying an effective response to the global crisis has required leaders to show strategic planning, coordination skills and the ability to communicate publicly their decisions in an empathetic manner. Also, maintaining a well-informed citizenry is essential in order to design a comprehensive approach and to reduce the significant health, security and social damage provoked by the COVID-19 crisis.

In the context of the Coronavirus pandemic, effective crisis communication applied by governments and international organizations may save lives and tackle the both sides of the crisis, potentially supporting the overcome of the *polychephalic threat.* Amid the viral powers of fake news, false information might cost lives and its implications may be more severe than the pandemic's.

Societies facing a crisis respond better when united – superior coordination and cooperation between governments, organizations, medical community, mass media and social networks is essential in terms of limiting the magnitude of the *polychephalic threat*.

The identified elements are just a few of a large range of measures national authorities, leaders and civil communities can undertake in order to fight "the Orthrus of the year 2020".

Last but not least, it is vital for the security environment to learn from the current pandemic and the infodemic around it. There are demanding lessons about trust, resilience and the complex security environment which surrounds us that can be drawn from the crisis situation, in accordance with the Latin proverb *eperientia docet*[30].

BIBLIOGRAPHY:

1. ***, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, Europol, 2020, URL: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
2. ***, *COVID-19: FAKE NEWS, 2020,* Europol, URL: https://www.europol.europa.eu/covid-19/covid-19-fake-news
3. ***, *A Guide to Open Government and the Coronavirus: Open Response + Open Recovery*, Open Government Partnership, 2020, URL: https://www.opengovpartnership.org/wp-content/uploads/2020/06/OGP-Guide-to-Open-Gov-and-Coronavirus.pdf

[29] Vital Strategies, *"Be Open, Honest and Proactive" – Global Experts Advise City Leaders on Risk Communication, Ethics and Legal Considerations during COVID-19 Pandemic*, 2020, URL: https://www.vitalstrategies.org/be-open-honest-and-proactive-global-experts-advise-city-leaders-on-risk-communication-ethics-and-legal-considerations-during-covid-19-pandemic/, accessed on 28.08.2020.
[30] Translation: „Experience is the best teacher".

4. ***, *Transparency, communication and trust: The role of public communication in responding to the wave of disinformation about the new Coronavirus*, Organisation for Economic Co-operation and Development, 2020, URL: https://www.oecd.org/coronavirus/policy-responses/transparency-communication-and-trust-bef7ad6e/#back-endnotea0z3
5. ***, *Policy Report – Fake News: National Security in The Post-Truth Era*, RSIS – S. Rajaratnam School of International Studies, 2018, URL: http://journres1.pbworks.com/w/file/fetch/135129183/Fake_News_National_Security_in_the_Post-.pdf
6. ***, *Is China winning the coronavirus response narrative in the EU?*, The Atlantic Council, 2020, URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/is-china-winning-the-coronavirus-response-narrative-in-the-eu/
7. ***, *Chapter Four: Metamorphosis*, The Department of Classics of the Ohio State University, n. d., URL: https://classics.osu.edu/sites/classics.osu.edu/files/Johnston_Metamorphosis_Chapter_ for_sharing_August_27_2015[1].pdf
8. ***, *The COVID-19 Infodemic: Combatting 'Dangerous' Misinformation on Social Media*,The Department of Communication of the Michigan State University, 2020, URL: https://comartsci.msu.edu/about/newsroom/news/covid-19-infodemic-combatting-dangerous-misinformation-social-media
9. ***, *COVID-19: Crisis Communications*, Tony Blair Institute for Global Change, 2020, URL: https://institute.global/sites/default/files/inline-files/Crisis%20Communications.pdf
10. ***, *DISINFODEMIC: Deciphering COVID-19 disinformation*, UNESCO, 2020, URL: https://en.unesco.org/covid19/disinfodemic/brief1
11. ***, *UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis*, United Nations, 2020, URL: https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19
12. ***, *"Be Open, Honest and Proactive" – Global Experts Advise City Leaders on Risk Communication, Ethics and Legal Considerations during COVID-19 Pandemic*, Vital Strategies, 2020, URL: https://www.vitalstrategies.org/be-open-honest-and-proactive-global-experts-advise-city-leaders-on-risk-communication-ethics-and-legal-considerations-during-covid-19-pandemic/
13. ***, *Munich Security Conference*, World Health Organization, 2020, URL: https://www.who.int/dg/speeches/detail/munich-security-conference
14. ***, *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*, World Health Organization, 2020, URL: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020
15. BRANDT, Philipp and WÖRLEIN, Jan, *Government crisis communication during the coronavirus crisis: Comparing France, Germany, and the United Kingdom*, 2020, URL: http://www.cso.edu/fiche_actu.asp?actu_id=2570
16. DEMPSEY, Judy, *Judy Asks: Is the Coronavirus Breeding Disinformation Across Europe?*, 2020, URL: https://carnegieeurope.eu/strategiceurope/81508
17. GELFERT, Axel, *Fake News: A Definition*, in *Informal Logic*, vol. 38, no. 1, pp. 84-85, URL: https://informallogic.ca/index.php/informal_logic/article/view/5068
18. GIGLIOTTI, Ralph A., *Leader as Performer; Leader as Human: A Discursive and Retrospective Construction of Crisis Leadership*, in *Atlantic Journal of Communication*, vol. 24, no. 4, Taylor and Francis, 2016.
19. GRZESIAK-FELDMAN, Monika, *The Effect of High-Anxiety Situations on Conspiracy Thinking*, in *Current psychology*, vol. 32, Springer Publishing, 2013.
20. GUNHILD HOOGENSEN, Gjørv, *Coronavirus, invisible threats and preparing for resilience*, 2020, URL: https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html

21. HOLMES, Aaron, *Facebook is launching a new 'coronavirus information center' that will appear at the top of people's News Feeds*, 2020, URL: https://www.businessinsider.com/facebook-coronavirus-information-center-news-feed-feature-covid-2020-3
22. JOWETT, Garth S. and O'DONNELL, Victoria, *Propaganda & Persuasion – Fifth Edition*, SAGE Publications, Thousand Oaks, 2012.
23. KULKARNI, Vaibhavi, *Is It the Message or the Medium? Relational Management during Crisis through Blogs, Facebook and Corporate Websites*, in *Global Business Review*, vol. 20, no. 3, SAGE Publications, Thousand Oaks, 2019.
24. NICKERSON, Raymond S., *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, in *Review of General Psychology*, vol. 2, no. 2, Education Publishing Foundation, 1998.
25. PACEPA, Ion Mihai and RYCHLACH, Ronald J., *Dezinformarea*, Humanitas, Bucharest, 2015.
26. PAMMENT, James, *The EU's Role in Fighting Disinformation: Taking Back the Initiative, 2020*, URL: https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286
27. YANG, Christopher C., CHEN, Hsinchun and HONG, Kay, *Visualization of large category map for Internet browsing*, in *Decision Support Systems*, vol. 35, Issue 1, Elsevier, 2003.
28. ZENELI, Valbona and SANTORO, Federica, *China's Disinformation Campaign in Italy*, 2020, URL: https://thediplomat.com/2020/06/chinas-disinformation-campaign-in-italy/

THREE FAMILIES OF CRISES SUPERPOSED, INTERDEPENDENTAND MUTUAL INTERFERING IN THE CORONAVIRUS CRISIS AND THEIR IMPACT ON THE INTERNATIONAL RELATIONS PERSPECTIVE

Iulian CHIFU, Ph.D.
Professor at "Carol I" National Defense University,
President of the Conflict Prevention and Early Warning Center, Bucharest, Romania.
E-mail: keafuyul@gmail.com

Abstract**:** *The Coronavirus or Covid-19 pandemic has launched a health crisis with an important impact by accelerating three categories of crises: the dormant and rampant ones that were here long before this crises; the correlated crisis coming from the pandemic explosion and the ways to limit its impact; and the independent crisis, not directly related by Covid-19 but prompted and accelerated by the pandemic. As a result, this lead to a maximum complication for the decision makers since it created overnight premises for a completely different International Relations Perspective. The scenarios for the world of tomorrow and the possible arrangement for a global governance are the aims of our study.*

Keywords: *pandemic; crises; interdependence; superposed; dormant crises; rampant crises; global governance.*

Disclaimer**:** *This assessment is made in the middle of the first wave of the crisis, when the number of cases was still increasing very fast. At this time, the prospects of the second wave, in autumn-winter, the coronavirus mutations, the prospects of safe treatment, or finding an effective vaccine are unknown. The prospect of perpetuating social/physical distancing measures may radically change the current assessment, so we reserve the right to return with revisions as knowledge of Covid-19 advances.*

1. Crisis and decision making in times of crisis

Crises are usually sudden changes on the evolution that prompt a threat to basic values, emergency and the sense of urgency in order to limit the effects and costs and to bring back the society at stake closer to the original situation[1]. Crises are accelerating the processes and trends that happened before or during the moment of emergence of the crisis. The coronavirus crisis is in the same situation and the changes in the society, politics and international relations are unpredictable and important.

The coronavirus pandemic has already brought major changes to human behaviour, society, politics, leadership, democracy, and the perspective of international relations. It is too early to name the outcome of the crisis in medical terms and time frame. But we already see interdependent and superposed crises as a result of the pandemic. It is, however important to try to foresee the possible way of managing the international world order after the crises, the

[1] Iulian Chifu, *Decizia în criză*, Editura Rao, 2019, ISBN 978-606-006-349-0, 335; Eric Stern, *Crisis Decisionmaking*, Stokholm University Press, 2001.

trends and alternative futures as well as the new shape of the post-pandemic geopolitics and World Order[2].

At the level of individuals and human society, the changes are relevant to the psycho-sociological dimension, the state of emergency and isolation at home creating various behaviours and ways of reaction. The repetition of this situation brings permanent changes in society, in multiplied individual preferences and behaviours, calibrated on the themes and directions of adaptation to the pandemic[3]. In addition, free time and the proximity of the computer and the Internet allowed the development of Infodemic, information warfare and propaganda, the uncontrolled spread of conspiracy theories, based on lack of facts and lack of societal cohesion, the absence of direct dialogue between members of society. Also, the inconsistency of the authorities, who were forced to communicate in times of crisis without exact data and clear information on Covid-19, amplified the conditions in which this Infodemic managed to spread.

At the level of society and politics, the coronavirus pandemic has revealed the strengths of democratic governments in the face of technological and social media developments, developments that have had an unexpected impact in promoting populism and extremist approaches, popularity, and overconfident and shocking claims, extraordinary speculation, even if unproven, against expertise, or a balanced approach. Against this background, the current pandemic has highlighted the need for serious and professional people to return to the forefront and the need for political elites - limited, blamed, and largely unacceptable in Western states – to reconnect with the natural and professional elites in society[4]. The recourse to expertise and the need for professionalism emerged, at the political level due to the credibility of the message for the public. Populism and extremism of all kinds didn't succeed in such times of crises, and people moved back in support of established classical ideological approaches and rationality. That were the means to cope with excessive emotionality, provoked and amplified through social media.

Although we do not know how long these changes will last and how permanent they will become[5], at the level of international relations there are great changes that show a shift in trade, economic and power relations with China, respectively its decoupling from global trade, with or without President Trump's re-election. In this context of overlapping crises, caused by the coronavirus crisis, authoritarian states and mainly those with populist leaders

---

[2] Iulian Chifu, "Noua geopolitică globală în era post-covid-19", in *Infosfera*, nr 2/2020, ISSN 2065-3395, pp. 3-15; Iulian Chifu, "Lumea post-Covid19. Impactul pandemiei asupra Rusiei și eșafodajului global", in Olivia Toderean, Segiu Celac, George Scutaru, *Lumea de mâine.Ce urmează după pandemie?*, Editura Curtea Veche, București, 2020, ISBN 978-606-44-0681-1, pp. 266-281; Iulian Chifu, „The impact of the Covid-19 pandemic on man, society, politics and International Relations", in Iulian Chifu, *The impact of the pandemic on the individual, society and global world*, Editura ISPRI, Bucharest.

[3] Iulian Chifu, *Spectrul pandemiei amenință umanitatea: psihoza Covid-19 în variate forme*, in Adevărul, 3 August 2020, URL: https://adevarul.ro/news/societate/spectrul-pandemiei-ameninta-umanitatea-psihoza-covid-19-variate-forme-1_5f26f51d5163ec42719a587d/index.html.

[4] Iulian Chifu, *Conducerea lumii de după COVID-19: schimbări și reașezări, bătălii și lovituri pe sub masa*, deschide.md, 10 April 2020, URL: https://deschide.md/ro/stiri/editorial/64298/Iulian-Chifu--Conducerea-lumii-de-dup%C4%83-COVID-19-schimb%C4%83ri-%C8%99i-rea%C8%99ez%C4%83ri-b%C4%83t%C4%83lii-%C8%99i-lovituri-pe-sub-mas%C4%83.htm; Iulian Chifu, *Bătălia publică, subterană și ocultă pentru conducerea lumii de după Covid-19*, Calea Europeană, URL: https://www.caleaeuropeana.ro/iulian-chifu-batalia-publica-subterana-si-oculta-pentru-conducerea-lumii-de-dupa-covid-19/; Iulian Chifu, *Renașterea dreptei. Reconectarea la elite*, 3 July 2020, URL: https://adevarul.ro/news/politica/renasterea-dreptei-reconectarea-elite1_5eff2ddb5163ec427198fe41/index.html

[5] Iulian Chifu, *Sfârșitul coșmarului: scenariile prospective pentru criza de coronavirus – pauza de 3 luni, îngheț un an sau amenințare eternă a omenirii,* Adevărul, 4 May 2020, URL: https://adevarul.ro/international/in-lume/sfarsitul-cosmarului-scenariile-prospective-criza-coronavirus-pauza-3-luni-inghet-an-amenintare-eterna-omenirii-1_5e86bdb55163ec427167438b/index.html.

seem to be the big losers in times of crisis, where the actions are the only thing that matters, and pursuing approval and benefits is punished by the public. China is the main target, through the guilt attributed to it and Donald Trump's new campaign strategy. And Russia, although it now has the opportunity to realign, is being pushed off the map to marginal areas of low crisis management, collateral error and the important impact of the crisis in the population, without any formal support from the central government, while President Putin's uncertain future makes it less present on the negotiation table of relevant aspects of the world of tomorrow.

2. Crisis as accelerators of trends

Crises have a very present effect on existing trends and on the pre-crisis crises, as well as on the third category, the independent crises emerged during the major pandemic. During a crisis, we can see a sudden process that shift the evolution of a day by day life and events. Crises are exposing, accelerating and amplifying the processes and trends, therefore creating secondary crisis, revealing creeping, rampant and dormant crisis on the making, in a process linked to the maximum complication in the current affairs.

For decision makers, there's a real headache to try to make sense in times of crisis. It happens because crises do not take numbers and never stay in line. They happen just like that and you need to solve them at the same time, with more or less the same resources as in normal times. Moreover, the crises are interfering one with the other, influencing themselves and creating conundrums where the solution should be addressed in an integrated manner, since an act to solve a crisis could harm and worsen the evolution of another one that happens in the same time.

Crises are, therefore, complex in nature. In turbulent times, there are numerous and therefore interact, being superposed, intertwined, mutually influencing one another. Moreover, since a crisis is creating an acceleration in the normal life, some other trends could become themselves crises over night, or secondary crises due to the original sudden change in the evolution.

In some other cases, the fact of accelerating trends and evolutions during crises creates a chaotic, random and unpredictable environment that accentuates and reveal crises that we weren't aware of before the original impact occurred. It is about the creeping crisis – developed in long periods of time – but first and foremost the dormant crisis as well as the rampant crisis, with a very small and unnoticeable evolution in normal times.

Moreover, besides those categories of crises prompted, revealed, accelerated or determined by the original crisis, the extraordinary dynamic in a social environment, crowded and influenced by numerous events and evolutions, new independent crises are emerging, without any direct link to the original event. These are not secondary crises, but most probable emerging crises, new independent crises, opportunistic crises because these are born, launched and developed due to the accelerated turbulences by the original events and the techtonics of the environment.

That's the way Covid-19, SARS-CoV2 or the coronavirus pandemic acted at the beginning of 2020, since the spread of the virus has been acknowledged at the global level. The coronavirus crisis has determined dramatic changes in the society, politics and international relations. As of today, it is too early to call and to decide what are the real consequences and the real impact of the pandemic on the world. We don't know yet the time frame of the crisis and in that environment, if we have **second waves and lock downs**, because the temporary changes that are repeating themselves tend to become permanent.

3. Three generations of crises

In that case, we can talk about three generations of crises prompted by Covid-19: the pre-crisis crisis, or the crisis already in evolution at the moment that the pandemic was acknowledge, including the rampant, dormant and creeping crises revealed by the acceleration of trends when the coronavirus emerged, the pandemic itself as a health crisis and its secondary crisis and the independent crisis that emerge in the chaos provoked by the pandemic, without any connection to the Covid – 19. All happened in the same time frame, and needed to be fixed, dealt with and solved at the same time by the same decision makers.

3.1 The pre-crisis crisis. The World in crisis

The Covid – 19 pandemic didn't happen in normal times. We already were in a highly turbulent environment, with a number of crises emerging and trends that were leading to new types of crises ready to appear. Moreover, some other trends were covering rampant and dormant crises that waited only the impact of the pandemic to explode, helped also by the accelerating trends and tendencies prompted by the impact of coronavirus.

The pre-crisis crisis – the generation of crises preceding the coronavirus pandemic – included those dormant or rampant crises determined by the impact of technology and especially social media on the individual, the society, the political life and the international relations. A big part of them were creeping crises, with a small increase of threat to basic values, the biggest part not perceived yet nor by the decision makers, neither by the public. A few academic writings were noticing already those changes and the impact and unintended consequences of those evolutions without any previous evaluation.

On another point, we already were in a period of trends towards ending the oil era, the change of the generation of energy production especially due to concerns linked to the Global Heating and environment as a whole. We already had in place international agreements, not only debates at an academic and scientific level. All lead to commitments at a political level, from Rio, Rio+10 and Paris, as well as public policies assumed at the level of the European Commission and some other states of the World.

In the same category we can put the savage globalization, its effects, consequences, reactions towards those evolutions and the need to manage it. Rampant crises were also the explosion of populism and extreme political ideas stepping in the forefront of the political life and in the Parliaments of the democratic states, due also to the support of social media in spreading with priority those ideas, an unintended consequence of the exponential development of social networks.

Moreover, the result of such a political anormality of the evolution of liberal democracy was the continuous fight, with debatable and questionable grounds, against the elite and expertise of the state, a split between the political elites and the professional and natural elites of the society. These crises were very visible during the pandemic when serious people and credible leaders were needed to explain and calm down the population, to lead efforts to cope with the crisis.

3.2 The secondary crisis of the pandemic

The coronavirus crisis has several aspects. The main problem is that it tests the leadership, as well as the political and administrative system of a state, not just the health system, in many ways. Especially since the coronavirus pandemic comes with multiple overlapping secondary crises, being, in fact, a crisis of multiple crises, in addition to the current medical predicament:

- the first is about the information warfare, propaganda, and exploitation of the crisis in the battles for prestige and image;
- the second is the crisis of confidence of the society, in itself, its leaders, decision-makers, and, at the same time, about panic, credibility and the crisis decision-making;
- the third is about leadership and the quality of the political class, political parties and political elites;
- the fourth is about the quality of liberal democracy in the social media and populism era, and an explosion of extreme ideologies being promoted versus professionalism, meritocracy and the return to the leadership of qualified elites in a society;
- let's not forget about the crisis and the resettlement of the medical/health system, with all its current strengths and imbalances, with the difficult examination it is failing today;
- last but not least, it's the global economic crisis caused by the coronavirus, including stress in supply chains, and the trade crisis, as well as the foreseeable decoupling of China from the US if not World trade.

The economic crisis seems the most important because it determines the readjustment of the world of tomorrow. With its existential threats, but also with opportunities to take control of global governance and the management of tomorrow's globalization[6].

So, we have a number of interdependent and superposed crises as a result of the pandemic, the secondary crisis of Covid-19, a multiplicity of crises:

- Medical crises. The illness;
- Health system crises. Capacity and evolution of the services;
- Infodemic to informational war. Who's to blame? Responsibility and opportunities to challenge liberal democracy from the position of autocracies. Prestige, image, perceptions;
- Society changes. Crisis of trust, credibility, capacity of the society to adapt and to cope with the crises, to absorb the changes in the day by day life imposed by lock downs and solutions to contain the crisis, including limiting human rights;
- Leadership crises;
- Political crises as a whole, prompted by the pandemic;
- Debate about the quality of liberal democracy, limits in times of crisis and the need to improve the reaction in exceptional times;
- Economic crisis.

4. Independent superposed trends and new emerging crises

As we have seen, it is about the new evolutions leading to new crises due to the chaos and turbulence determined by the pandemic. Those new crises are happening in the same time frame as the pandemic coronavirus crisis, but are not linked to neither as a direct secondary crisis. They are just the consequence of the acceleration of trends and, somehow, they are some type of oportunistic crises.

In this category or generation of crises we can talk about:

- The end of the Nuclear Era (as we know it) due to the operationalisation of laser weapons and the public tests of intercepting airplanes and missiles. At the same time, the end

[6] Iulian Chifu, *Testul suprem pentru Regimul Dodon: pregătirea de criza Covid-19 și credibilitatea conducerii de la Chișinău*, Adevărul, 1st April 2020, at https://adevarul.ro/moldova/politica/testul-suprem-regimul-dodon-pregatirea-criza-covid-19-credibilitatea-conducerii-chisinau-1_5e8363bc5163ec42715755a1/index.html; deschide.md, March 31, 2020, at https://deschide.md/ro/stiri/editorial/63637/IChifu--Testul-suprem-pentru-Regimul-Dodon-preg%C4%83tirea-de-criza-Covid-19-%C8%99i-credibilitatea-conducerii-de-la-Chi%C8%99in% C4%83u.htm

of nuclear weapons control treaties and their limits via existing international control treaties made nuclear actors loose a superiority or automatic recognition of some special rights at the international/global level. Both evolutions happen just during the pandemic.

- The end of the Cold war inheritage occurs by consequence, transforming Russia from a global super power, inheriting USSR nuclear arsenal and international position, into a medium regional power, according to its economic resources, the contribution to global trade, research and progress as well as perceived image. Its fall was develop in pair with the raise of China as a global challenger to the US power and its long term global position as unique superpower, after the fall of the Soviet Union.
- The end of the oil. A change of the generation of energy. Moving towards clean energy. The previous creeping crisis that we registered in the pre-crisis crisis marked it's critical point during the pandemic, as an independent crisis, after the Russian-Saudi war for oil price and markets, at the end of the two years moratorium of production, after the rejection by Russia of the new OPEC plus agreements.
- The revival of cosmic travels and conquest of the Moon and Mars, together with the development of space anti-satellite military weapons, was also an evolution acknowledged during the pandemic.

5. International relations and Global Security in the world of tomorrow

All those changes and superposed generations of crises lead to the conclusion that we could face a real reboot of the World of Tomorrow. For sure, the debate is still open if we will have a transformation, an adaptation, a genuine change, or a reform, if not a revolution, or even an implosion of the World Order as we know it. Due to the existing level of culture and knowledge, thinkers and counselors of public figures involved in the debate, we would bet more on a conservative evolution rather than a revolutionary one, on the short to middle term, since there are not so many revolutionary ideas in the debates of scientists and practitioners, nor very numerous high level personalities able to dramatically change the world, and even not a concrete and visible will to act in that direction.

This comes with the rivalry already exposed in public between autocracies and liberal democracies, who's the best model, which countries reacted better in times of pandemic crisis. The battle of the alternative systems entered a very public phase with a lot of instruments used to convince the public, first and foremost Infodemic and informational warfare.

The whole effort for strategists and planners in international relations and global security lies in the possibility to foresee the possible way of managing the international security environment after the crises, to identify the trends and alternative futures in the next year or two as well as identifying the scenarios for the new shape of the post-pandemic geopolitics and World Order. A complex endeavour, with a high level of risk and error.

Our study reveals that the global governance possible formats for coping with the international crisis are the following:

- The G0 world – of no one, No One's World – the anarchic world without leadership, after Trump's USA withdrawal from the world scene. If not in splendid isolation, in a more self-preoccupied posture; – "America first, Great again!" – rather than ensuring global leadership.

- Returning to the world with US leadership – even if more nuanced, changed, and with more limited tasks, with or without the current president, with or without the current US leadership.

- The G2 world, the globalized world along the main lines of the big players, the USA and China. If they get along. If rivalries and the prospect of confrontation fade. If they collaborate. If China accepts the rules and follows them. If they don't end up fighting. Or at least ~~I~~ it? don't break the global trade, polarizing it into two sides, as they started to do. Slim chance! It would take at least half a miracle for this, or major global pressure.

- The US-China-EU tripod – which is rather an European ambition, a visionary assumption of Emmanuel Macron on the global role of the EU between the two seas, balancing them, but without the resources and agreement of the European economic engines. Again, it is difficult to predict the likelihood of this scenario in the short and medium-term.

- P5 - the group of permanent members of the Security Council, as leaders in the debate on the future of the world and the management of globalization. Again, with very big differences in quality of life, manners, fundamental values, and specific weight between the actors and with major differences between them. But with an initiative already on the table - Macron-Trump-Putin. We will see the leaders of the action, and their directions, if this initiative will actually work.

- G7 (G8) - is a natural framework for discussing the major issues of the world, the G8 variant being the desire and aspiration of Russia, which is not in the category of the most industrialized states in the world, but yearns its global role.

- G20 - a broader framework, which blurs the ambitions and trends of the Great Power policy that all the other projects so far reveal. It was proposed as a sketch in a letter published as an editorial in The Washington Times by Mevlut Ceavusoglu, Turkey's foreign minister. This is also a *pro domo* plea, but it has its substance and relevance[7].

Our analysis has led to several scenarios, none of which are likely to be good and salutary in the current context. All of them bring to the fore rather the continuation/acceleration of globalization as an objective process, and the effects of the coronavirus crisis on the populist, nationalist, and isolationist options, which we will analyse below.

- *Worst case scenario* remains the politics of power - i.e. the inclination to use force, war, aggressive influence to achieve political goals, respectively the policy of Great Power - i.e. the temptation of a Great Deal between the great powers, inclined to share world domination, which also means multipolarism, spheres of influence and privileged interests. The world will be divided and deals will be made between great powers, behind closed doors, regarding the future of these spheres of influence. Unfortunately, this is a scenario likely to materialize.

- *Best case scenario* remains the arrangement of the world based on multilateralism, the rule of law, a world based on rules, consensualism in decisions (technically, the EU values extrapolated globally). While it is promising, the probability of heading in this direction is very low given today's world and the political leaders we inherited, which must guide the current world through the coronavirus crisis.

- *The most likely scenario* oscillates between two variants, and these on the good-bad scale: The G0 world, anarchic, without leadership, with rivalries between great powers and, why not, possible wars, with inadequate ambitions and leaders in the forefront, and with the abandonment/marginalization of professionalism and meritocracy, but leaning towards partitocracy and the closure of democratic systems; or Transatlantic Leadership - if it manages

[7] Iulian Chifu, *Criza de coronavirus, Globalizare, politică de Mare Putere și Concertul Mondial*, in Adevărul, 5-6 April 2020, at https://adevarul.ro/international/in-lume/criza-coronavirus-globalizare-politica-mare-putere-concertul-mondial-5-1_5e89eab25163ec427175a514/index.html; Iulian Chifu, *Bătălia publică, subterană și ocultă pentru conducerea lumii de după COVID-19*, in Adevărul, 9 April 2020, at https://www.caleaeuropeana.ro/iulian-chifu-batalia-publica-subterana-si-oculta-pentru-conducerea-lumii-de-dupa-covid-19/.

to overcome the poor management of the crisis, populism, the temptation to change unfavorable narratives, with a possible change of leadership or options for the main actors, and the need to coordinate global efforts in line with civilized, Western, democratic states.

If the transatlantic rift that many are forcing ends up closing, the United States will no longer be the leader we know, it will need the general support and legitimacy of the contribution of all democratic states in the transatlantic community. It is a simple, well-known, beaten and functional road, it has its own common values at its base, it is easy to rebuild, maybe with other leaders, and the will and support of the population can be catalyzed because the need is obvious[8].

Unfortunately, the possible catalyst for such a scenario, both likely and close to a best-case, includes the use of the common enemy trope to catalyze all the support, namely the designation of China as a common enemy! American documents and many documents from the European and EU Member States are beginning to contain converging elements in such a direction.

Conclusions

So the most probable constant elements in any scenario of the world of tomorrow are:

- a US-China polarized world, with a high possibility of a split of the trade and political partners of the two and a high level of constrains on third states to align one way or the other and with a few actors really independent and immune to the dispute;
- old and new rivalries are going to re-emerge and last, with more or less intensity;
- a full debate at a political level will emerge about the type of response and responsibility in crises;
- China's behaviour will be subject of debate as well as its responsibilities in the pandemic crisis.

Options and scenarios would align according to those lines:

- limiting US-China divergences and a capacity to deal with the rivalry. The formation of a G2 format to solve the big issues of the world and lead the globalization (more probable if Biden becomes the President of the United States);
- US confronting China – China as an enemy with a genuine consecutive polarization of the world;
- a Chinese – American ongoing rivalry, developed below the radar. Limited confrontation – economy, trade, decoupling, relocation. Ambiguity in presenting those relations clearly and at every moment. The world would be closer to anarchy – G0 world than to G2 global governance. The solutions will be searched and applied in regional frameworks and through local deals.

The New Global Geopolitics will have three main characteristics:

- A Dissipated power – less power at a level of one player, the need of alliances and global deals in order to manage the globalisation and solve the global issues and fundamental problems of humanity.
- A Chinese-American constant rivalry – with ups and downs, more or less visible and harmful, depending on the internal events, elections and power evolution.

[8] Iulian Chifu, *Criza de coronavirus, Globalizare, politică…*

- The need and inclination towards consensual multilateralism, a system where the EU has extensive experience in finding consensus between multiple actors and supporting a rules based international system.

BIBLIOGRAPHY:

1. CHIFU, Iulian, „Lumea post-Covid19. Impactul pandemiei asupra Rusiei și eșafodajului global", in Olivia Toderean, Segiu Celac, George Scutaru, *Lumea de mâine.Ce urmează după pandemie?*, Editura Curtea Veche, București, 2020, ISBN 978-606-44-0681-1
2. CHIFU, Iulian, „Noua geopolitică globală în era post-covid-19", in *Infosfera*, nr 2/2020, ISSN 2065-3395.
3. CHIFU, Iulian, „The impact of the Covid-19 pandemic on man, society, politics and International Relations", in Chifu Iulian, *The impact of the pandemic on the individual, society and global world,* Editura ISPRI, București, în curs de apariție.
4. CHIFU, Iulian, *Bătălia publică, subterană și ocultă pentru conducerea lumii de după Covid-19*, Calea Europeană, https://www.caleaeuropeana.ro/iulian-chifu-batalia-publica-subterana-si-oculta-pentru-conducerea-lumii-de-dupa-covid-19/
5. CHIFU, Iulian, *Bătălia publică, subterană și ocultă pentru conducerea lumii de după COVID-19,* in Adevărul, 9 April 2020, at https://www.caleaeuropeana.ro/iulian-chifu-batalia-publica-subterana-si-oculta-pentru-conducerea-lumii-de-dupa-covid-19/
6. CHIFU, Iulian, *Conducerea lumii de după COVID-19: schimbări și reașezări, bătălii și lovituri pe sub masa*, deschide.md, 10 April 2020, https://deschide.md/ro/stiri/editorial/ 64298/Iulian-Chifu--Conducerea-lumii-de-dup%C4%83-COVID-19-schimb%C4%83ri-%C8%99i-rea%C8%99ez%C4%83ri-b%C4%83t%C4%83lii-%C8%99i-lovituri-pe-sub-mas%C4%83.htm
7. CHIFU, Iulian, *Criza de coronavirus, Globalizare, politică de Mare Putere și Concertul Mondial,* in Adevărul, 5-6 April 2020, at https://adevarul.ro/international/in-lume/criza-coronavirus-globalizare-politica-mare-putere-concertul-mondial-5-1_5e89eab25163ec427175a514/index.html.
8. CHIFU, Iulian, *Decizia în criză*, Editura Rao, 2019, ISBN 978-606-006-349-0.
9. CHIFU, Iulian, *Renașterea dreptei. Reconectarea la elite*, 3 July 2020, https://adevarul.ro/news/politica/renasterea-dreptei-reconectarea-elite-1_5eff2ddb5163ec427198fe41/index.html
10. CHIFU, Iulian, *Sfârșitul coșmarului: scenariile prospective pentru criza de coronavirus – pauza de 3 luni, îngheț un an sau amenințare eternă a omenirii,* in Adevărul, 4 May 2020, URL: https://adevarul.ro/international/in-lume/sfarsitul-cosmarului-scenariile-prospective-criza-coronavirus-pauza-3-luni-inghet-an-amenintare-eterna-omenirii-1_5e86bdb55163ec427167438b/index.html
11. CHIFU, Iulian, *Spectrul pandemiei amenință umanitatea: psihoza Covid-19 în variate forme*, in Adevărul, 3 August 2020, URL: https://adevarul.ro/news/societate/spectrul-pandemiei-ameninta-umanitatea-psihoza-covid-19-variate-forme-1_5f26f51d5163ec42719a587d/index.html
12. CHIFU, Iulian, *Testul suprem pentru Regimul Dodon: pregătirea de criza Covid-19 și credibilitatea conducerii de la Chișinău*, in Adevărul, 1st April 2020, at https://adevarul.ro/moldova/politica/testul-suprem-regimul-dodon-pregatirea-criza-covid-19-credibilitatea-conducerii-chisinau-1_5e8363bc5163ec42715755a1/index.html
13. CHIFU, Iulian, *Testul suprem pentru Regimul Dodon: pregătirea de criza Covid-19 și credibilitatea conducerii de la Chișinău*, deschide.md, March 31, 2020, at https://deschide.md/ro/stiri/editorial/63637/IChifu--Testul-suprem-pentru-Regimul-Dodon-preg%C4%83tirea-de-criza-Covid-19-%C8%99i-credibilitatea-conducerii-de-la-Chi%C8%99in%C4%83u. htm
14. STERN, Eric, *Crisis Decisionmaking,* Stokholm University Press, 2001.

THE IMPACT OF THE COVID-19 PANDEMIC ON NATIONAL AND INTERNATIONAL SECURITY

Viorel ORDEANU, Ph.D.
Colonel (ret.), M.D., Professor, Senior Researcher,
Medical-Military Scientific Research Center, Titu Maiorescu University, Bucharest, Romania.
E-mail: ordeanu_viorel@yahoo.com

Lucia Elena IONESCU, Ph.D.
M.D., Researcher, Medical-Military Scientific Research Center, Titu Maiorescu University, Bucharest, Romania. E-mail: ionescu.lucia@gmail.com

Abstract*: Transmissible infectious diseases are caused by living biological agents that can be transmitted in different ways from the source, causing outbreaks, epidemics or pandemics. The current epidemiological situation, the COVID-19 pandemic is serious due to its rapid transmissibility, strong complications, and the fact that it is an unknown disease. Given its characteristics, similar in parts to a biological agent used as a disabling weapon, in this paper we will address the current COVID-19 pandemic as an ongoing "situational experiment" in order to simulate a targeted biological attack (on a strategically important locality) with infectious effects that extends nationally and internationally. This type of pandemic has destructive potential through the created health crisis, followed by the economic crisis, aggravated by the information crisis (infodemics) and finally the social crisis with unpredictable consequences.*

Keywords*: security; pandemic; COVID-19; health crisis; economic crisis; situational experiment; medical intelligence; fake news.*

Introduction

Infectious diseases are caused by living biological agents (bacteria, viruses, fungi, parasites, etc.) that can be transmitted in different ways from the source (sick individual, sick animal, biological weapon or contaminated environment) causing outbreaks, epidemics or pandemic. The current epidemiological situation, the COVID-19 pandemic caused by the new SARS-CoV-2 coronavirus is serious due to its transmissibility, complications (viral pneumonia with lethal potential), the fact that being a previously unknown disease makes as the specialists do not yet master the clinical pathology, epidemiology, therapy, prophylaxis and possible social and economic consequences. SARS-CoV-2 characteristics made of it a proper subject for a „situational experiment" (unwanted, unprovoked but useful for practical study and training) in order to identify medical and non-medical countermeasures against a possible biological attack.

1. The new international health emergency: COVID-19; a multifactorial analysis

1.1. General situation

At the beginning of December 2019, against the background of the exacerbation of respiratory viruses, some more serious cases, complicated by viral pneumonia, were

registered in Wuhan City (Chinese Republic). Laboratory tests showed that there was no flu, no Severe Acute Respiratory Syndrome (SARS) or Middle East Respiratory Syndrome (MERS), but another newly discovered coronavirus. It was originally called the New Wuhan coronavirus or New Chinese coronavirus. Then, in January 2020, it became known as nCoV 2019, not to make reference to the geographical area. The World Health Organization (WHO) has recommended the provisional name of the disease to be *"2019-nCoV acute respiratory disease"* and in February, the official name COVID-19 for the disease and SARS-CoV-2 for the virus was established. This disease is a viral zoo-anthroponomics, hitherto unknown, which spreads directly inter-humanly, with high contagiousness, similar to the flu. The measures, both medical and non-medical, to combat this epidemic are special in scope and extent. There are still many questions related to this viral disease, which are waiting for the most urgent answers as the clinical pathology, therapy, diagnosis, prophylaxis, microbiology, epidemiology, and public health, but also related to its impact from social, economic, political, military and other perspectives.

The epidemic of SARS-CoV-2 that causes the COVID-19 disease has spread, despite extreme anti-epidemic measures, unparalleled in medical history and has become a pandemic. One cause to the increase in the number of cases and contamination was the massive influx of people from infected countries and areas. The disease is new, the etiological agent was not previously known, so all we know about it is only by analogy, and through empirical observations and ongoing scientific research. As a result, the first infectious cases from November 2019 were misdiagnosed, and in December when the disease was identified and an epidemic was declared, there were no specific reagents for diagnosis, specific antiviral drugs and no vaccine for prophylaxis. Medicine has progressed rapidly, faster than in any other epidemic, but the spread of the virus, which has proven to be extremely contagious, has outpaced anti-epidemic measures, so in the first quarter of 2020 a pandemic was declared. In the meantime, some countries have overcome the peak of the epidemic, but in the European Union and the United States it continues to spread thus for the second quarter and the third quarter of the year no further evolution can be predicted.

The writer Mark Twain, a journalist by profession, said: "If you don't read the newspaper, you're uninformed. If you read the newspaper, you're misinformed". We have the written and audio-visual press as well, that is literally bombarding us with bad news about the novel coronavirus, COVID-19, epidemic, pandemic, treatments, diagnoses, deaths, hospitals, etc. Even more recently, news are about the economic crisis (which had begun anyway), with all its consequences until the depression, probably greater than that of the twentieth century. Companies of all sizes are closing, we have unemployed people of all kinds, pupils and students no longer go to school. Social distancing is the order of the day, circulating on foot or with vehicles is conditioned, restrictions are differentiated by social categories or age. Public gatherings are mainly prohibited. Many people are isolated at home, quarantined or hospitalized even if they are asymptomatic. In some countries, the police, gendarmerie and army organize filters and patrol the streets, intervening by force whenever necessary. All those who violate these restrictions are fined with significant amounts of money or arrested, for "thwarting anti-epidemic measures"[1].

1.2. The clinical situation

Clinical symptoms begin trivially. Many individuals are contaminated without being sick, but there is a suspicion that they could transmit the infectious agent through direct contact. Most of those infected have a ***mild***, febrile ***form*** of viral respiratory infection that can

[1] ***, *Ordonanţă de Urgenţă nr. 28 din 18 martie 2020 pentru modificarea şi completarea Legii nr. 286/2009 privind Codul penal*, Art. 352 (In English: Romanian Government Ordinance no. 28 /2020, 352 Article).

be treated at home with conventional medication. Furthermore, the patient's immune system has specific and non-specific anti-infective defense mechanisms and most patients recover. So far, the situation is like the flu or an Upper Respiratory Tract Infection (URTI) (cold, influenza, etc.) which are often caused by other coronaviruses. However, there is still no evidence that the clinically cured patient is at risk of transmitting the virus or not. As with the flu and other severe coronavirus diseases, such as SARS or MERS, some patients develop ***serious complications*** with viral pneumonia, altered general condition and even death. Elderly people are at risk primarily because they have a less effective immune system, as well as very young children because they have not yet fully developed their immune defence systems. Then there are the chronically ill people (heart disease, pulmonary disease, obese, etc.) who find it more difficult to bear the decompensations caused by the viral infection, the congenitally immune-deficient people with acquired deficiencies of the immune system as a result of infections (for example, HIV/AIDS) and radiation, of toxic or immunosuppressive drugs (after organ transplantation, autoimmune diseases or as a side effect) or persons biologically debilitated due to physiological or pathological causes.

All of these patients should be hospitalized for confirmation of diagnosis, isolation, appropriate complex treatment, including antivirals, and specific intensive care. But some of these patients die. Even if the registered mortality is very low, if one considers the high contagion, the virus will lead to a significant number of diseases and deaths. Here one can make a comparison with the flu, a relatively mild viral infectious disease, as it is said in medical folklore "the untreated flu lasts 7 days, and the treated only one week". If effective public health measures are not applied (surveillance, vaccination, diagnosis, isolation, treatment, etc.), the contagiousness is high and the lethality low. So far, it seems that nothing is surprising or "scary" for experienced doctors. Obviously, none of us have the experience of the "Spanish flu" pandemic, which was actually brought from Hong Kong. Not even the most developed countries in the world would cope with this situation, with the forces and sanitary means at their disposal. Moreover, it can be assumed that the countries that apply the health insurance system would be completely overwhelmed in case of a biological crisis (with a natural or provoked epidemic). But in reality, as a result of medical and non-medical measures, it is observed, for example, that the current flu epidemic in Romania caused in December 2019-February 2020 over 7,000 clinical cases, of which approx. 1,700 were confirmed by the laboratory through molecular biology and only 40 patients died from the flu. The result is an average mortality of approx. 0.5%, common in the flu.

All personnel involved in the transport, diagnosis and/or treatment of patients suspected of having the COVID-19 infection should be vigorously protected. It is not only about their health and wellbeing, their families and those around them, their patients, but also about public health in general if they become secondary sources of contamination. We must not rely on the "professional immunity" that repeated contact with various pathogens gives us over time, because in the case of a new microorganism there is no such protection. The most important aspect, valid in any serious epidemic, is that the medical staff must remain healthy and fit for work, in order to perform their duty to the population. If there is a shortage in qualified staff to care for the sick people, the epidemic can become catastrophic and can rapidly evolve into a biological crisis. Not coincidentally, health personnel are considered a risk group.

1.3. Microbiology

Viruses isolated from patients and animals were examined by electron microscopy and, thus, could be observed the specific structure of the pleomorphic virion's halo of spikes (crown shaped). Genomic sequencing was successful, proving this coronavirus to be different

than those already known (SARS, MERS, etc.). Cultivation was performed and animal models were developed for drug and vaccine research as well as for the study of the contagion. Estimations have been made: moderate contagion; mortality below 3% (so below SARS and MERS), vaccine time, at least one year[2] (some experts have estimated two years, others six months, and pessimists never, so everything is relative).

As of February 25th, it has been reported that several virus strains have been identified in the 93 samples analysed by molecular genetics, with a known haplotype for hemagglutinin (H1, H3 and H13) and two new ones (H56 and mv2) in Wuhan, as well as two older (H13 and H38) in Shenzhen and Washington (USA) that were not identified in Wuhan patients. The conclusion is that there are distinct sources, that the epidemic has been in general circulation since November, and that Wuhan is not the only source, but there are multiple. So at least three different roots of contamination can be identified[3].

In December 2019, after the discovery of this novel coronavirus, it was found with concern that the medical systems of the world do not have specific antivirals, vaccine and specific reagents to fight the disease. Virology and pharmaceutical laboratories in China and around the world immediately began scientific research on the novel virus. The results of the research and the evolution of the cases were communicated on the Internet, some even on the day of their obtaining, which represents an absolute scientific premiere.

1.4. Epidemiology

We do not know the exact source of the current outbreak of coronavirus disease 2019 (COVID-19), but we know that it originally came from an animal, likely a bat[4].

The epidemiological investigation established that the first cases were related to the animal market in Wuhan, and the animal and fish markets in the area were immediately closed and decontaminated. Accordindly with WHO in early February in China were 11821 confirmed infection and 259 deaths.[5] Wuhan is the largest city in central China, about six times as big as Bucharest, the largest industrial centre and has direct connections with the European Union through airlines, railways and roads. The evolution of the epidemic was monitored on a daily basis, according to WHO press releases broadcasted on the Internet. Italy with great connections with China was the first EU country to declare quarantine, and on 25.02.2020 there were 323 confirmed cases with 11 deaths, so 3.4% mortality rate. After this date, it seemed that the number of new cases was decreasing in China, so the epidemic had exceeded the maximum and entered into remission. Paradoxically, there are no epidemic in children, only isolated cases. But expansion outside of China has created the risk of a pandemic, especially in countries where social discipline is low and where the authorities' health recommendations are not being followed.

In the massmedia, both the power and the opposition, but also the "independent", appear predominantly similar with the official point of view, without deviations. Even in the US, the pro-Trump and anti-Trump massmedia present the situation similarly, but in contradiction with the WHO and scientific publications. Following the news, one cannot understand who stimulates the dissatisfaction (leading even to street fights) and for what

[2] Flora Graham, "Coronavirus Outbreak", *Nature Briefing*, 2020 Springer Nature Limited, February 3rd, 2020, URL: https://www.nature.com/ articles/d41586-020-00297-w, accessed on 12.08.2020.
[3] ***, *Les scientifiques chinois ont remonte la piste du coronavirus en Chine*, Reseau International, 25 Fevrier 2020, URL: https://reseauinternational.net/les-scientifiques-chinois-ont-remonte-la-piste-du-coronavirus-en-chine/, accessed on 12.08.2020.
[4] ***, *COVID-19 and Animals*, Center for Disease Control and Prevention, 24 Augusut 2020, URL: https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/animals.html, accessed on 29.09.2020.
[5] ***, Covid-19 Situation Report, 01.02.2020, URL: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200201-sitrep-12-cov.pdf?sfvrsn=273c5d35_2, accessed on 29.09.2020.

purpose. Is the purpose to spread of the epidemic (for evil purposes) or to avoid the economic crisis (for beneficial purposes)? Or, there are all sorts of mixed interests and more or less spontaneous reactions.

This, hereby, is an attempt to look at things and facts objectively, from a scientific perspective, not with the purpose of showing support or an attempt to thwart something, but only to understand what the truth is and what we are all heading for, driven *en masse*, energetically and convergent. *The National Health Federation, a Non-Profit Health Freedom Organization since 1955* (NHF) published an interesting documentary in late April 2020. The NHF President, Scott C. Tips was awarded by the *International Academy of Oral Medicine & Toxicology* (IAOMT) for the conference and the article "*Never Has So Little Done So Much Harm to So Many. The Latest Coronavirus Attack Is Cover for Restricting Our Health Freedoms*". He recalls that the WHO declared the COVID-19 pandemic in February 2020 arguing, among other things, that the disease has a mortality rate of 3.4% compared to the seasonal flu 0.1%; but the author says the comparison is not correct because different formulas were used, and for COVID the light cases that solve on their own were not taken into account. If the same calculation rule applies, the seasonal flu is twice as lethal as COVID-19 In fact, the Internet presents the official situation on a daily basis and it is clear that the majority of COVID-19 cases are mild or asymptomatic (*Worldometer coronavirus*[6]). As a comparison, the seasonal flu epidemic in Europe, in 2017, was much more deadly than in 2020, and the mortality peak was double, but no isolation or quarantine (MMVR) was imposed and no one was "scared" and now the number of respiratory infections decreased compared to the same period of the year[7]. If this formula is applied, the mortality in Wuhan was only 0.04-0.12%, but the problem is that in a very large population this percentage means a very large number of patients who crowd the hospitals and some died. Never in the history of medicine have such drastic and extensive measures been taken, not even in the most lethal viral epidemics. *"So, why now"?* The author wonders, and points out that the US risks destroying its economy and the American and international financial markets which are mainly based on the USD.

It can be seen that at the beginning of this century most epidemics, especially viral ones, were poorly estimated and the reality did not confirm the scientific predictions, although most of us had no specific reagents for diagnosis, recommended therapy or vaccine. Then, the question remains: *Who carries the interest?*

1.5. Public health

The epidemic of the novel coronavirus began and was declared in December 2019, on the eve of the biggest holiday of the Chinese people: the Chinese New Year, the period in which over 300 million Chinese in the country and around the world travel to celebrate with their families. And more than 7 million Chinese were preparing to fly to 400 cities in more than 100 countries, but Chinese authorities have stopped flying so that the epidemic does not become a pandemic[8]. In any modern country the health of the population is guaranteed by the state that is obliged to take all necessary measures in this respect, with or without foreign aid. The Chinese government has resolutely imposed the necessary measures, of an unprecedented

[6] ***, *COVID-19 coronavirus pandemic*, URL: https://www.worldometers.info/coronavirus, accessed on 29.09.2020.
[7] Scott C. Tips, "The latest coronavirus attack is a cover for restricting our health freedoms", *Publisher's Corner,* Nordskog Publishing Inc, June 3rd, 2020, URL: https://www.nordskogpublishing.com/the-latest-coronavirus-attack-is-a-cover-for-restricting-our-health-freedoms/, accessed on 12.08.2020.
[8] ***, Nature 577, 450, 2020, URL: https://www.nature.com/articles/d41586-020-00153-x, accessed on 29.09.2020.

severity and magnitude in the history of medicine. And the WHO expects effective, tailor-made measures from all Member States.

An interesting case is presented by an American cruise ship, with thousands of people on board, where the epidemic broke out; the ship was quarantined in Japan, but some foreign nationals (including Romanians) were repatriated at their request[9].

2. Non-medical effects of the health crisis[10]

2.1. Economic effects

Any epidemic disrupts the economic and social life. Contrary to the WHO's recommendations not to restrict trade and travel in relation to China, some states have introduced restrictions that affect not only China's economy but also those of other countries, even though it is a well-known fact that this country, which is the world's second largest economy, is also called "The factory of the world".

A positive factor is that scientifically applied medical research has suddenly been stimulated for the emergency production of diagnostic reagents: kits for the novel virus and others for differential diagnosis. There is an ongoing process for the manufacture of new antiviral drugs and specific vaccines, on medical equipment for anti-infective protection (for which China provides about 90% of the world's needs), etc. The pharmaceutical industry will grow and make huge profits. German virologist Rolf Hilgenfeld, who is experienced in SARS, immediately moved to Wuhan to study the virus on the spot, in order to test active compounds in experiments on animals as candidate drugs for human treatment. If confirmed, clinical trials will take approx. 6 months more.

The new epidemic coming from China is seen as a favourable opportunity for some to contain the boom of the Chinese economy, to block trade and travel to and from China as much as possible, to block the expansion of the "Silk Road" to the Euro-Atlantic area and to make an economic defence against the "yellow danger". But also to justify the imminent economic crisis/depression of the western world through the "effects of the epidemic". The epidemic also serves as a pretext for the exorbitant spending of "prevention" through massive investments in the private pharmaceutical industry.

2.2. Social effects

Any epidemic has negative effects, not only on the life and health of the population, but also on the social and economic life, causing disruptions proportional to the severity of the epidemic and the lack of response of the authorities. On January 30th, 2020, when there were already thousands of patients and hundreds of deaths worldwide, but the vast majority in China, the WHO declared the novel coronavirus epidemic a *public health emergency of international concern* (PHEIC). It is the highest level of sanitary alarm, as interpersonal transmission outside China had already been confirmed. WHO Director-General, Tedros Adhanom Ghebreyesus, stressed that this statement is not a vote of no confidence in China, as some countries have suggested, and said "It is time for solidarity, not stigma".[11] He also praised China for its anti-epidemic measures and recommended that trade and travel to and

[9] ***, *COVID-19 outbreak: Commission supports repatriation of EU citizens from cruise ship in Japan*, European Commission Press Release, 19 February 2020, URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_296, accessed on 29.09.2020.

[10] Viorel Ordeanu, "COVID-19 pune armate de oameni in miscare", *Viata Medicala*, no. 9 (1569), 6 March, 2020, pp. 1, 8.

[11] James Chau, „A time for solidarity, not stigma", *China Daily*, 06.02.2020, URL: https://www.chinadaily.com.cn/a/202002/06/WS5e3bd44da31012821727587f.html, accessed on 29.09.2020.

from China not to be restricted. But PHEIC is a valid alarm for all countries and they are obliged to strengthen their sanitary measures and prepare for potential cases.

The unlikely hypothesis of taking China out of the world trade circuit could have disastrous effects not only for the Chinese population but globally, as the flow of cheap Chinese goods has led to an increase in living standards in almost all countries. The sudden interruption of this flow, the shortage of products and the high prices could lead to discontent and mass riots in many states, causing social unrest of varying intensity and with unpredictable consequences.

2.3. Political effects

The novel epidemic has also sparked an "information war", with major multinational-controlled Western media outlets criticizing everything related to the epidemic and China, and the so-called "independent" press praising the effectiveness and scale of sanitary measures taken by Chinese authorities. Most journalists present the facts as alarmingly as possible, the pharmaceutical industry is preparing for a new financial "boom" (after the real pandemics and those missed in recent years). It is obvious that the public, instead of being informed, is misinformed, and mass media (written and audio-visual) becomes a source of partisan controversy, with implications on the national and international security. We consider the scientific press, especially *Nature* (Springer) and *Science* (Elsevier) from the US, the most prestigious scientific publications in the world, present objective and balanced facts and data, based on updated statistics and medical experiences, as well as the statements of WHO specialists.

However, because both the virus and the disease are new and there is still no medical experience in managing the epidemic, any further evolution is possible, from the rapid remission of it, statistically observed in China, to the pandemic spread to all inhabited continents and the evolution for at least two years. Thus, on February 24th, cases and deaths were confirmed in several countries, on all continents, including Europe[12]. The EU was also hit hard by the epidemic wave and its aftermath, and Romania was no exception. It is interesting to note that some countries have already overcome the health crisis and are in the process of economic recovery, either by authoritatively imposing restrictions (e.g. China, Vietnam, South Korea, etc.) or on the contrary, by not imposing restrictions (Sweden, Japan etc.).[13]

2.4. Military issues

Along the multiple criticisms brought to the Chinese authorities, an unproven hypothesis was launched that the virus was a biological agent that escaped from the laboratory. It is known that Wuhan, the most important urban and industrial centre in central China, is home to the national equivalent of the *Centre for Disease Control* (CDC China), which also has a high-security microbiology laboratory (BSL4) controlled by the military and by China's Academy of Science. If it were a biological weapon, it would fall into the category of "disabling" (the mortality ranging from 1 to 3%) and at the same time its use as an "ethnic weapon" because it selectively attacks the Chinese, so it would not be created by them. As a result, the dispute ended.

---

[12] ***, „Coronavirus latest: WHO says outbreak is not yet pandemic", *Nature*, Springer News, 24.02.2020, URL: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200224-sitrep-35-covid-19.pdf?sfvrsn=1ac4218d_2, accessed on 29.09.2020.

[13] Andrew Korybko, "The NYT is waging information warfare by politicizing the coronavirus", *CGTN*, 09.02.2020, URL: https://news.cgtn.com/news/2020-02-09/The-NYT-is-waging-information-warfare-by-politicizing-the-coronavirus-NWN51fK1JS/index.html, accessed on 11.08.2020.

The imposition of extended quarantine in the Wuhan region required specific forces and means, including military and non-military. In a few days, four thousand military doctors and paramedics were brought to strengthen the sanitary measures, hospitals were created in public buildings, new hospitals with thousands of places were built, and sanitary materials were brought with the military aviation. Thousands of soldiers were brought in to maintain order and quarantine. It is worth remembering that in the great cholera epidemic at the beginning of the last century in Romania, the area of Brăila was quarantined, at the request of Professor Cantacuzino; and the gendarmes prevented the people from fleeing, in an extreme case by shooting, so as not to spread cholera throughout the country.

On February 14th, it was announced that the US military was preparing for a possible coronavirus pandemic, although there were only 15 cases of COVID-19 in the United States at the time. But the order was for the military to be prepared in the event of an epidemic and for the army to be able to carry out its missions, including for the imposition of quarantine[14]. In fact, this type of training is useful for any pandemic and for biological defence in case of an attack with biological warfare agents or bioterrorism.

2.5. Medical intelligence

We consider some reliable and objective sources on the situation of the COVID-19 epidemic are the WHO Geneva and CDC Atlanta (USA) information releases as well as the scientific publications (which publish editions in print and/or electronic form). If the multitude of available medical information would be analysed, one could see the slips, intentional or forced, statistical or data interpretation errors, masked advertising for reagents, drugs, vaccines, protective equipment and prophylaxis measures, as expensive as possible, as extensive as possible, as profitable as possible for the pharmaceutical industry. Personalities from the medical and political world also fell into the trap, as well as some prestigious publications (e.g. *Lancet Gate*).

The main prophylactic measures, in the absence of better ones, remain: avoiding agglomerations, face mask-wear both by the sick not to spread the virus and by the healthy not to inhale the virus, washing hands with soap and water both after and before any actions, drastic sanctioning of those who cough or sneeze in public without protection, isolation of patients (minimum 2 weeks), immediate examination and treatment of any person with signs of respiratory virus infection, control teams in airports, railway stations, ports, bus stations, subway and strict epidemiological surveillance of the population.

3. The health crisis as an apparent trigger of the economic crisis and insecurity

3.1. Updates

Today, as Eminescu used to say: "Everything is old and everything is new". As of March 20th, China had 81,000 confirmed patients, with virtually no new cases, with 3,253 deceased, 70,420 cured and the rest still under treatment[15]. Symbolically, the medical staff took off their masks in an *ad hoc* ceremony. The draconian measures applied by the Chinese authorities, the devotion of the medical staff and their population's discipline saved the nation and gave time and example to other countries to take protective measures, if they wanted to

[14] ***, "Les militaires americains se preparent a une eventuelle pandemie de coronavirus", *Observateur Continental*, 17.02.2020, URL: http://www.observateurcontinental.fr/?module=news&action=view&id=1383, accessed on 13.08.2020.

[15] ***, *Coronavirus disease 2019 (COVID-19) Situation Report – 60*, World Health Organization, URL: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200320-sitrep-60-covid-19.pdf?sfvrsn=d2bb4f1f_2, accessed on 26.09.2020.

and if they could. The Director-General of the WHO, Ethiopian Doctor in Biology and an experienced politician, has repeatedly emphasized this medical success and insisted that no reference be made to ethnicity or geographical area in the name of the disease and of the pathogen. The recommendation was that all efforts to be directed, convergent, to combat the epidemic. The WHO has formalized this attitude and called on all member states to implement the most appropriate measures immediately.

After the new change in terminology, the "severe acute respiratory syndrome" viral disease newly called COVID-19 was declared an epidemic in December 2019, and the novel virus was called SARS-CoV-2, meaning "severe acute respiratory syndrome coronavirus 2". Meanwhile, this virus has been spreading in Asia, then in Oceania, America, Europe, and Africa, practically on all continents and in almost all countries. After being declared by the WHO as an "international public health emergency for public health", when the epidemic spread to several countries, with interpersonal transmission outside China, a **pandemic** was declared. In China the prevalence was higher, but mortality was lower. In the European Union, the epidemic is still ongoing, all data are on an upward slope and the necessary measures are being taken very late. The Italians have proved unable to stop the epidemic. In our case, even though we are trying, we cannot stop the mass repatriation of contaminated Romanians, we missed the first orders of specific materials and the doctors "in the front line" do not have sufficient means of protection and massively get sick.

3.2. Prevalence

Regarding the real prevalence, there is a problem of statistical interpretation, related to the case definition. Considering that this viral disease, like other coronaviruses, usually manifests itself as a trivial Upper respiratory tract infection (URTI), asymptomatic or very mild cases go almost unnoticed, the mild ones are not medically registered (Romanians are champions in self-medication and empirical treatments), it seems that all these seemingly healthy people could be the source of contamination. Cases with moderate or severe symptoms reach the doctor, are recorded, as appropriate, as influenza, COVID-19, etc. and are treated at home or in hospital. So the real prevalence of the disease is yet unknown, which in extreme circumstances could contaminate the entire population. If we made a graphical representation of this hypothetical situation at the level of the country's population (a very unlikely apocalyptic scenario) we would theoretically have a pyramid in geometric regression, which would include almost all the inhabitants.

3.3. Diagnosis

As with any infectious disease, the clinical diagnosis must be supplemented with a microbiological diagnosis. No one could test the entire population, nor would it be necessary. However, the following categories must be tested: suspects (feverish people and those with Upper respiratory tract infection - URTI), contacts (accidental or family) and risk groups (health personnel, civilians and military working to combat the epidemic, medically vulnerable people and dignitaries) and healed patients (to confirm healing). For healthy people without the risk of contamination, testing would be useless, time consuming, effort and means that could be used for the sick. The national need for testing would be in the order of millions.

The diagnosis tests can be done in two ways:

- By *reverse-transcription Real Time PCR* which is a high precision diagnostic method that offers the possibility to identify the causative agents of infectious diseases by identifying their genetic material in samples obtained from the person under investigation. The microbiological diagnosis is so accurate that the identification of the virus is also the

confirmation of the diagnosis. But the method is so sensitive that the result can appear positive also in the case of the virus already defeated, which no longer causes the disease.

- By *immunological method* (faster and cheaper), that detect specific antibodies, but is considered only a screening method for diagnosis, which must be confirmed in case of positivity, with molecular biology analysis. But, the antibodies are formed by the sick patient's body only after contact with the infectious agent; therefore, it shows a belated diagnosis of the disease, or that the body has once gone through the disease and has achieved immunity or that it has been vaccinated. It is very important for the clinical situation, but less for intervention in the epidemic.

3.4. Contagiousness

It has been shown that the SARS-CoV-2 virus is transmitted directly, through the air (through Flugge micro droplets from the sick patient) but also through contamination of the environment with secretions that contain the virus, and it is relatively resistant to the environment (hours or days). Moreover, the patient also eliminates viruses through the stool (COVID-19 is a respiratory disease that also affects the intestine). Therefore, the virus can be found in toilets, floors, objects, hands (becoming a "dirty hand disease" as the gastrointestinal infections such as diarrhoea, so with secondary "faecal-oral" transmission). This means that precautions must be taken simultaneously for air transmission and direct and indirect contact.

Individuals who carry the virus without being sick (the contaminated and the asymptomatic) can contaminate healthy people and become *secondary sources of infection*. But infected people have a bi-univocal relation between the host organism and the pathogenic microorganism, through which they develop immunity and are no longer receptive. When the majority of the population will have an active immunity (going through the disease in a symptomatic or asymptomatic manner, or through vaccination) the epidemic shall enter into decline and shall disappear "on its own". However, the big problem is that all those who are vulnerable in that respective population (the chronically ill, the elderly, and the immune-deficient persons) will get the disease in serious or even lethal form. As Charles Darwin postulates, "natural selection" intervenes, which unfortunately for medicine, really works.

This should not be treated lightly. In the civilized world we live in, there is a significant share of the elderly (many of which are still socially active) and the long-lived, we have many chronic patients or with severe bio-psycho-social sequelae, who are kept alive due to the remarkable advances of modern medicine. We all have a degree of biological distress due to "modern life": stress, artificial food, illicit and licit drugs (smokers, drinkers, etc.) that undermine our health. All this could also explain why in "Old Europe" and in the US this pandemic seems to be more serious: we have many more vulnerable people, susceptible to disease and complications.

One of the most prestigious scientific journals in the world, *Springer Nature* (USA) published the *News Nature Briefing* on March 19, comparing COVID-19 with other infectious-contagious diseases we face today. Thus, COVID-19 has a mortality rate slightly above seasonal influenza and the pandemic influenza A (H1N1) since 1918, but well below SARS, tuberculosis, avian influenza A (H7N9), MERS, Ebola, etc., and the disease is less infectious than seasonal influenza and many other infectious diseases. Therefore, from a medical perspective there is nothing to be afraid of, but we must get seriously involved in prevention, diagnosis, treatment and recovery. Nevertheless, the world is panicked, with the interested or disinterested (but not uninterested) contest of governments, multinationals, experts or a certain part of the written and audio-visual press, which stand as holders of the only truth, considering any other opinion as "fake news". Thus, we may wonder whether the intented or unintended governmental fake news have the role of supporting national security

or not. Even some scientific publications participated in the launch of "fake news", citing only the *Lancet Gate* scandal that led to the retraction of a falsified study on COVID-19 treatment[16] or the statements of some WHO experts that led to the US withdrawal from this organization. Overall, the COVID-19 epidemic caused a pandemic followed by an economic, financial and social crisis, being exacerbated by an "infodemic". Among the contradictory fake news, the real news get lost, which makes for a difficult selection thereof, especially since many are or seem official. The President of the United States, Donald Trump, in his speech on July 19th, 2020 (also presented by Romanian television channel B1TV at 7 pm) drew attention, among other things, that: "The new far-left fascism demands absolute allegiance"[17]. If we look at the world situation objectively, we have a different vision of the public health (see Worldometer 2020). But the great risk of the present is that we do not yet have the experience of the new epidemic and we do not know how far it will spread and what the consequences will be.

A possible explanation for the exaggerated measures against the real danger to public health would be the hypothesis that the new coronavirus could be a biological agent for a new disabling biological weapon, which we do not yet know well enough.

Doctor Faucci, Director of the *Centre for Diseases Control (CDC Atlanta, USA)* predicted the "surprise" of an epidemic coronavirus 3 years ago. In September 2019, a biological defence exercise, *"Event 201"*, took place at the *John Hopkins Centre for Health Security* (New York), which was also attended by Bill Gates, and the hypothetical virus was called "n-Cov"[18]. In November, cases of viral pneumonia appeared in the city, some lethal, and in December 2019 the novel coronavirus was identified, originally called n-Cov. It was supposed to have spread from the animal market in Wuhan, from various animals: bats, cats, etc. The direct transition from animal (wild or laboratory) to human is a controversial topic. But different strains have been identified in different parts of the world, in humans and animals, suggesting a multiple origin, and in addition, different paths of transmission have been identified. At least 5 different strains of SARS-CoV-2 have been found, so the sources are multiple, the circulation of the virus is older and the disease has probably been neglected so far, not being diagnosed correctly. French virologist Luc Montagnier (Nobel laureate in HIV identification) concluded that the new virus was an artificial hybrid between a coronavirus and HIV, made in the laboratory for a possible HIV vaccine and accidentally escaped. And suddenly this real but not major danger comes first and the entire Euro-Atlantic civilization is blocked by national and supranational authorities: *"It is as if someone gave machine guns to a troop of chimpanzees".*[19]

Former Israeli Health Minister Professor Yoram Lass said "isolation kills more people than the virus"[20] and Swiss infectious disease doctor Pietro Vernazza argued that this isolation

---

[16] M. Chossudovsky, *Lancet-Gate: Scientific Corona Lies and Big Pharma Corruption. Hydroxychlorochine versus Gilead's Remdesivir*, Global Resarch, Canada, July 6th, 2020, URL: https://www.globalresearch.ca/scientific-corona-lies-and-big-pharma-corruption-hydroxychloroquine-versus-gileads-remdesivir/5717718, accessed on 06.07.2020.

[17] Federico Finchelstein, „Trump's Mount Rushmore Speech Is the Closest He's Come to Fascism", *Foreign Policy*, 8 July 2020, URL: https://foreignpolicy.com/2020/07/08/trumps-mount-rushmore-speech-fascist-politics-zeev-sternhell/ accessed on 26.09.2020.

[18] ***, *Statement about nCoV and our pandemic exercise*, John Hopkins Center for Health Security, URL: https://www.centerforhealthsecurity.org/news/center-news/2020-01-24-Statement-of-Clarification-Event201.html, accessed on 28.09.2020.

[19] Scott Tips, *Never Has So Little Done So Much Harm to So Many. The Latest Coronavirus Attack Is Cover for Restricting Our Health Freedoms*, Nordskog Publishing, 3 June 2020, URL: https://www.nordskogpublishing.com/the-latest-coronavirus-attack-is-a-cover-for-restricting-our-health-freedoms/, accessed on 28.09.2020.

[20] Hadas Magen, "Lockdown lunacy", *Globes*, 22 March 2020, URL: https://en.globes.co.il/en/article-lockdown-lunacy-1001322696, accessed on 28.09.2020.

and other restrictive measures are not science-based and should be lifted, except for vulnerable groups (depending on pre-existing diseases)[21]. The president of the *World Doctors Federation*, Frank Ulrich Montgomery, said that isolation measures in Italy are unreasonable and counterproductive. The Swedish health authorities have not restricted anything (but have made recommendations to the population) and consider that the severe measures are only a "*political placebo*"[22].

The overall press creates and maintains fear and hysteria of the pandemic, by constantly presenting data about the disease, the ill and the deceased, about the serious social and economic implications. There are already cases of confirmed patients who commit suicide, there are terminally ill patients with the diagnosis of death as COVID-19, there also is medical staff who flee from duty, and businessmen who take advantage of the situation. The Secretary of State at the Ministry of Health, Doctor Moldovan, stated on a TV station on 05.05.2020 that "80% of the deaths attributed to COVID-19 have other causes of death"[23]Now all self-conscious and/or psychopathic "benefactors" and "experts" launch catastrophic or conspiratorial hypotheses and give advice, including therapeutic ones. And the pharmaceutical industry "Big Pharma" and even some in the medical world see this pandemic and consider it a "financial boom" regardless of the human, social, economic and financial costs for the population it has to protect. However, we also have realistic, firm voices: "we are interested in the trend, not the number"[24], as stated on TV by Doctor Raed Arafat, head of the Romanian Department for Emergency Situation.

From a medical perspective, rabies is a very rare viral disease, but extremely dangerous because the mortality is of 100% so we must pay maximum attention to it. No infectious disease should be underestimated, but the measures taken should be proportionate to the risk. The interviews and statements of some professors, reputable specialists, who are far from the general hysteria caused by this coronavirus could be easily added, but we must look for them carefully in the multitude of news and *fake news*. Even the president of the country advises us to listen only to the official news and to beware of fake news, but it is precisely these that have the greatest public outcry. It is no coincidence that the image that illustrates Scott Tips' documentary symbolically shows a person throwing his TV out the window.

3.5. The reality

Almost all governments have a desperate need to blame someone or something for entering the impending recession. Which, in fact, has been announced for several years by the leaders of the world economy, including us, by the Governor of the National Bank of Romania, Mugur Isarescu. It is worth remembering that even though TV stations broadcasted after the Military Ordinance no. 1 that "We have everything we need"? and immediately after the Military Ordinance no. 2 that "Doctors should request everything they need", it became

[21] Juergen T Steinmetz, "The Risk of Dying on Coronavirus? COVID-19 Research tells the truth", *eTurbo News,* April 1, 2020, URL: https://www.eturbonews.com/568969/risk-of-dying-on-coronavirus/, accessed on 28.09.2020.

[22] Kebour Ghenna, "The Corona crisis is a media crisis", *Meda News,* 10 April 2020, URL: https://news.meda.chat/2020/04/10/the-corona-crisis-is-a-media-crisis/, accessed on 28.09.2020.

[23] ***, "Ar putea fi refăcut bilanțul deceselor de Covid-19 în România? Precizările secretarului de stat Horațiu Moldovan", *Digi24*, 05.05.2020, URL: https://www.digi24.ro/stiri/actualitate/sanatate/ar-putea-fi-refacut-bilantul-deceselor-de-covid-19-in-romania-precizarile-secretarului-de-stat-horatiu-moldovan-1302349, accessed on 28.09.2020.

[24] Corina Chiriac, "Raed Arafat vine cu informația momentului! Valul unu încă nu s-a terminat!", *Capital*, 24 iulie 2020, URL: https://www.capital.ro/raed-arafat-vine-cu-informatia-momentului-valul-unu-inca-nu-s-a-terminat.html, accessed on 28.09.2020.

necessary for the release of Military Ordinance no. 3 to involve the army for providing support and for ensuring compliance with the anti-epidemic recommendations. And it was necessary for the National Anticorruption Directorate to make order in the procurement of medical protection equipment[25].

It would be foolish to deny the pandemic, but one must also take into account the informed but contrary opinions of genuine specialists, whistle-blowers and integrity signallers, scientists who objectively interpret existing data to know the real level of risk and correctly base the prevention measures. Otherwise, people risk getting into more serious situations through the economic crisis than through the health crisis itself. As in any other treatment, curative or prophylactic, it must be applied the Hippocratic principle: "*Primum non nocere*" (first, do no harm).

For any infectious disease that can be fatal, people must guard against and follow official recommendations, but this does not mean abandoning critical thinking and social resignation, but on the contrary. And if population "stays at home", the national interest must not be neglected, because it concerns everybody, directly and indirectly. Especially, people should not to let themselves be absorbed only by daily worries so as not to lose the overview of the society they belong to. And people must understand where illness situation is manipulated and who can use the mystification regarding the severity of this disease.

But, nevertheless, there are some people in the world who are looking forward to the crisis. Unprecedented measures of austerity and social discipline will be taken, and the money will be used more or less wisely. But the risk for social-economic perspective is that the poorest to become even poorer, and the rich to become even richer. This has been the case with all crises and recessions, including the most recent, which began in 2008.

Conclusions

It turns out that although it is a medical crisis endangering the public health in all countries of the world, the most serious consequences of COVID-19 will be economic, by interrupting the activity in the industry and services sectors, international trade and international relations, which can deteriorate to trade war or even "hybrid war", with declining the living standards of the majority of the population and unpredictable social consequences.

We hope that through the national effort, through the sacrifice of the medical personnel, through the civil-military cooperation (CIMIC) provided in NATO regulations, with the application of the Solidarity Clause provided in the Charter of the European Union, with the technical support of the World Health Organization, with the involvement of local communities and with the discipline of every responsible citizen, to stop this epidemic and to recover economically, financially and socially. Success will depend on social discipline to comply with the recommendations, which in this situation are mandatory and will contribute to the strengthening of national security as part of the international security. Although, the statistical analysis of the COVID-19 situation, therefore objective, does not prove the correctness of the imposed measures. It starts from some epidemiological realities and reaches measures that can be seen as extreme, exaggerated, unnecessary or even harmful for the population in the short, medium and long term.

[25] *Ordonanţe militare 1-8/2020*, Ministerul Afacerilor Interne (In English: Military Ordinances 1-8/2020, Ministry of Interior).

BIBLIOGRAPHY:

1. ***, "Les scientifiques chinois ont remonte la piste du coronavirus en Chine", *Reseau International*, 25 February 2020, https://reseauinternational.net/les-scientifiques-chinois-ont-remonte-la-piste-du-coronavirus-en-chine/
2. ***, *Ordonanţă de Urgenţă nr. 28 din 18 martie 2020 pentru modificarea şi completarea Legii nr. 286/2009 privind Codul penal*
3. ***, *Romanian Military Ordinances 1-8/2020*, Ministry of Interior.
4. ***, *WHO Coronavirus Disease (COVID-19) Dashboard*, https://www.worldometers.info/ coronavirus
5. CHOSSUDOVSKY, M., „Lancet-Gate: Scientific Corona Lies and Big Pharma Corruption. Hydroxychlorochine versus Gilead's Remdesivir", Global Resarch, Canada, July 6th, 2020, https://www.globalresearch.ca/scientific-corona-lies-and-big-pharma-corruption-hydroxychloroquine-versus-gileads-remdesivir/5717718
6. GRAHAM, Flora, "Coronavirus Outbreak", Nature Briefing, 2020 Springer Nature Limited, February 3rd, 2020, https://www.nature.com/ articles/d41586-020-00297-w
7. KORYBKO, Andrew, „The NYT is waging information warfare by politicizing the coronavirus", *CGTN*, 09.02.2020, https://news.cgtn.com/news/2020-02-09/The-NYT-is-waging-information-warfare-by-politicizing-the-coronavirus-NWN51fK1JS/index.html
8. ORDEANU, Viorel, "COVID-19 pune armate de oameni in miscare", *Viata Medicala*, nr. 9 (1569), 6 March 2020.
9. TIPS, Scott C., "The latest coronavirus attack is a cover for restricting our health freedoms", Publisher's Corner, Nordskog Publishing Inc, June 3rd, 2020.
10. *Capital* website, www.capital.ro
11. *Center for Health and Security* website: www.centerforhealthsecurity.org
12. *Centers for Disease Control and Prevention* official website: https://www.cdc.gov
13. *China Daily* magazine website: https://www.chinadaily.com.cn
14. *Digi24* website, www.digi24.ro
15. *eTurbo News* website, www.eturbonews.com
16. *European Commission* official website: https://ec.europa.eu
17. *Foreign Policy* website, https://foreignpolicy.com
18. *Globes* website, https://en.globes.co.il
19. *Meda News* website, https://news.meda.chat
20. *Nature* magazine website: www.nature.com
21. *Observateur Continental* website, http://www.observateurcontinental.fr
22. *World Health Organization* official website: https://www.who.int

DIGITAL DISINFORMATION IN THE CONTEXT OF COVID-19 AND THE IMPACT ON GLOBAL PUBLIC HEALTH

Dana DRUGĂ
Ph.D. Candidate, "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania.
E-mail: sirbu.ionela@animv.eu

Abstract: *The purpose of this article is to analyze, based on the scientific literature, the main effects on global health security of the spread of disinformation about COVID-19. At the same time, this article illustrates how digital disinformation poses the risk of canceling credible sources, which can lead to mass public confusion and an increased risk of spreading and transmitting the virus. The objective of this article is to provide an overview of the current trends and insights into disinformation activities related to COVID-19/Coronavirus.*

Keywords**:** *disinformation; fake-news; COVID-19; conspiracy theories.*

Introduction

Coronavirus is a new type of virus that has not been previously identified in humans. This new type of coronavirus, called COVID-19, was not previously detected before the outbreak was reported in Wuhan, China in December 2019. More precisely, "coronavirus disease 2019 (COVID-19) is a respiratory tract illness resulting from infection with severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2); in recent months, COVID-19 has become a global pandemic, posing a major public health challenge for the health systems of many nations."[1]

As COVID-19 turned completely into a common health crisis, a lot of theories about the source of the virus have been circulating on the social media, all with a universal theme, that the virus was artificially fabricated in a laboratory by a deceitful government with a certain plan. Disinformation comes from social media platforms and sites without any scientific authority. These posts have garnered recognition and support, and theories continue to gain importance and be shared on the Internet, despite scientists from several countries analyzing the COVID-19 virus and concluding that the virus originated in nature, more precisely from an animal source.

What is the infodemic? According to the World Health Organization, the COVID-19 outbreak and the corresponding response have been accompanied by a massive infodemic, that is, by an excessive amount of information - in some cases correct, in others not - that makes it difficult for people to find trustworthy sources and guidance when they need it. The term *infodemic* refers to a large increase in the volume of information related to a particular topic, which can become exponential in a short period due to a specific incident such as the current pandemic[2]. In this situation, disinformation and rumors appear on the scene, together

[1] Samia Tasnim, Md Mahbub Hossain, Haimonty Mazumder, Impact of Rumors and Misinformation on COVID-19 in Social Media, *Journal of Preventive Medicine & Public Health*, 2020 May; 53(3): 171–174, URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280809/.
[2] *2020. Coronavirus Disease 2019 (COVID-19) Situation Report – 13*, World Health Organization, Geneva, Switzerland.

with the manipulation of information with dubious intentions. In the information age, this phenomenon is amplified by social media, spreading further and faster, like a virus.

What is disinformation? Disinformation is false or incorrect information for the deliberate purpose of misleading. According to Merriam-Webster Dictionary, disinformation is "false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth"[3]. In a pandemic, disinformation can negatively affect human health. Many false or misleading stories are made up and spread without verifying their truthfulness or quality. Much of this disinformation is based on conspiracy theories, and some of it introduces some of the elements of them into the mainstream discourse. Inaccurate and false information has been circulating about all aspects of the disease, such as the origin of the virus, the cause, the treatment and the mechanism of spread. Disinformation can spread and be assimilated very quickly, leading to behavioral changes that can lead to people taking greater risks. All of this makes the pandemic much more serious, harming more people, and jeopardizing the sustainability of the global health system[4].

The greater access in the world to mobile phones with internet connection and to social networks has led to the exponential production of information and the possible ways to obtain it, creating an information epidemic or infodemic. In other words, we are facing a situation in which a lot of information is produced and exchanged in all corners of the world, reaching billions of people.

1. Russian and Chinese disinformation in Europe

According to a study[5], the disinformation about Covid-19 broadcast by the Russian and Chinese media attracts more audience on social networks in Europe than the content of certain major newspapers. The Oxford Institute analyzed for three weeks the content produced by the main Russian and Chinese media channels, as well as the Iranian and Turkish media, controlled by the state or closely linked to the governing regimes of those countries. The study focused mainly on the Russian television channel RT, the Sputnik news agency, the Chinese Television Network, Radio China International and the China news agency.

In their publications in French, German or Spanish, these media channels politicized the coronavirus by criticizing Western democracies, praising their countries of origin and promoting conspiracy theories about the origins of the virus, according to the Oxford Institute. The report measures user engagement based on the number of redistributions, likes, or comments on Facebook and Twitter. The study covers the 20 most popular articles in each news station, from May 18 to June 5[6].

RT's French content gets an average engagement of 528 on Facebook and Twitter, and China 374, compared to 105 for the newspaper "Le Monde". In German, RT articles have a score of 158 on Facebook and Twitter, compared to 90 for Der Spiegel.

---

[3] Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/disinformation.

[4] Understanding the infodemic and misinformation in the fight against COVID-19, *PAHO*, URL: https://iris.paho.org/bitstream/handle/10665.2/52052/Factsheet-infodemic_eng.pdf?sequence=14, accessed on 24.08.2020.

[5] Katarina Rebello, Christian Schwieter, Marcel Schliebs, Kate Joynes-Burgess, Mona Elswah, Jonathan Bright, Philip N. Howard, *Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users. Understanding Chinese, Iranian, Russian and Turkish Outlets*, Data Memo 2020, Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk, URL: https://comprop.oii.ox.ac.uk/research/covid19-french-german-spanish/, accessed on 24.08.2020.

[6] *Idem.*

Jonathan Bright, a researcher at Oxford declared that most of the content on these channels is based on facts." But what they have, especially if you look at the Russian outlets, is an agenda to discredit democratic countries".[7]

"The subtle weave in the overarching narrative is that democracy is on the verge of collapse"[8], he added.

Previous research by the institute, published in April, has already highlighted the penetration of these media channels in English-language markets, revealing that some of their articles could reach levels of user involvement up to ten times higher than those of the BBC example. Similar levels of involvement have been observed in Spanish-language content, especially for the Iranian Hispanic media Hispan TV, which the report says promotes anti-American sentiment for Latin American users. "A significant portion of social media is people consuming content that is directly funded by foreign governments, and it's not very clear to the reader that that's the case", concluded Jonathan Bright.[9]

Researchers at the Oxford Internet Institute have isolated three main themes transmitted by these publications: on the one hand, the destabilization of Western democracies. RT France and RT Germany, for example, spoke of a silent demonstration against the Belgian prime minister or even anti-isolation demonstrations in France, Germany or Poland. The Chinese press, led by Xinhua, has questioned the credibility of American leaders, citing a "political virus". On the other hand, the same publications highlighted the positive aspects of the countries that control them, especially the Chinese media. "Xinhua's French and Spanish articles have highlighted international praise for China's poverty reduction initiatives among coronavirus solutions", the study said. The same model was used by the Turkish channel TRT, which celebrated a new hospital inaugurated by Turkish and Japanese officials in Istanbul, positioning the city as an international center for medical care. Only Russia has lagged behind in this regard[10].

2. Pro-Kremlin disinformation – overview of currently trending false narratives

The wave of disinformation that accompanied the coronavirus pandemic has been described as an unprecedented one, a real "infodemic" that has spread mainly through social media, which does not mean, however, that no other means have been used, including traditional media, and in this case, the EU vs. Disinformation, a programme launched in 2015 by the European External Action Service to combat Russian disinformation, found that the pro-Kremlin media was involved in the spread of pandemic disinformation. The European External Action Service found that no fewer than 550 such narratives were spread by pro-Kremlin sources. Narratives are intended to exploit the anxieties generated by pandemic and isolation and lead to confusion and distrust in the authorities, which ultimately undermines not only European institutions but also the efforts of health authorities.

---

[7] Press From, "Study: Distorted Chinese, Russian virus news takes root in West", URL: https://pressfrom.info/us/news/world/-469008-study-distorted-chinese-russian-virus-news-takes-root-in-west.html, accessed on 06.09.2020.

[8] *Idem.*

[9] Press From, "Study: Distorted Chinese, Russian virus news takes root in West", URL: https://pressfrom.info/us/news/world/-469008-study-distorted-chinese-russian-virus-news-takes-root-in-west.html, accessed on 06.09.2020.

[10] Katarina Rebello, Christian Schwieter, Marcel Schliebs, Kate Joynes-Burgess, Mona Elswah, Jonathan Bright, Philip N. Howard, "Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users. Understanding Chinese, Iranian, Russian and Turkish Outlets, Data Memo", 2020, Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk, URL: https://comprop.oii.ox.ac.uk/research/covid19-french-german-spanish/, accessed on 24.08.2020.

A report[11] by the European External Action Service (EEAS), which assists the EU High Representative for Foreign Affairs and Security Policy in the exercise of his mandate, reveals the scale of global disinformation, a phenomenon with potentially harmful consequences for public health and communication. According to the report, originally published on March 16 and later updated in the EU and other regions, coordinated disinformation messages seek to point to vulnerable minorities as the cause of the pandemic and encourage distrust of the ability of democratic institutions to provide effective responses.

Russia and China, as well as figures supported by these states, are accused of trying to exploit the public health crisis to promote geopolitical interests, questioning the credibility of the European Union and its partners. The report also claims that since the end of January, there have been more than 150 cases of pro-Kremlin misinformation about the new coronavirus. Among the fake news propagated is the one regarding the collapse of the European Union, due to a deficient response of the national governments in the coronavirus crisis. "Russian state-controlled media outlets have shifted their focus to highlight Russia's preparedness to tackle the outbreak. Russian aid to Italy was extensively covered"[12].

"The EU is not coping with the pandemic; The Union is about to collapse" are headlines promoted by pro-Kremlin sources, but also by other governments and internal networks / sources in EU Member States or even African countries. "The EU is selfish and betrays its own values". According to the EEAS Report, these ideas are promoted by pro-Kremlin sources, but also in other regions. In Ukraine, for example, catastrophic messages about an imminent collapse of the European Union are combined with the portrayal of Ukraine as a "false state" that has been abandoned by "European allies"[13].

3. The most popular conspiracy theories regarding COVID-19

The uncertainty, fear and complexity of the COVID-19 pandemic fueled the conspiracy theories. They were trying to explain why the pandemic occurred and who benefits from it. A global study conducted in 28 countries shows that more than 3 in 10 respondents believe that a foreign power or other force is deliberately causing the spread of the COVID-19 virus[14]. EU experts[15] point out that conspiracy theories often appear as a logical explanation for events or situations that are difficult to understand and bring a false sense of control. This need for clarity is exacerbated in times of uncertainty such as the COVID-19 pandemic.

Conspiracy theories also often start as a suspicion. The idea of who benefits from the event or situation appears and thus the conspirators are identified. Any "evidence" is then forced to fit the theory. Once they take root, conspiracy theories can grow rapidly. These are hard to disprove because anyone who tries is seen as part of the conspiracy. At the same time, experts say that most believe that conspiracy theories are true. Others deliberately want to provoke, manipulate or target people for political or financial reasons. Attention: they can come from several sources, e.g. internet, friends, relatives.

---

[11] *EEAS Special Report: Disinformation on the Coronavirus – Short Assessment of the Information Environment*, March 19, 2020, URL: https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/, accessed on 24.08.2020

[12] *EEAS Special Report Update: Short Assessment Of Narratives And Disinformation Around The Covid-19 Pandemic*, EU vs. Disinfo, April 01, 2020, URL: https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic/, accessed on 24.08.2020.

[13] *Idem.*

[14] ***, *The Coronavirus: A Vast Scared Majority Around The World, Snap poll in 28 Countries*, Gallup International Association, March 2020, URL: https://www.gallup-international.com/wp-content/uploads/2020/03/GIA_SnapPoll_2020_COVID_Tables_final.pdf, accessed on 24.08.2020.

[15] European Commission, *Identifying conspiracy theories*, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en, accessed on 24.08.2020.

Misleading information about COVID-19 is circulating in various ways – via social media, online messaging services. The World Health Organization has also been warning for some time that the outbreak and reaction to COVID-19 is accompanied by an "infodemic"; "an over-abundance of information – sometimes accurate and sometimes not – that makes it difficult for people to find reliable sources and guidance when they need it"[16]. This misleading information is also sometimes disseminated by people without any objective of harming public debate, democratic processes, the open economy or national security.

More than 100 false theories about the new coronavirus are circulating worldwide, according to a team of researchers at Carnegie Mellon University in the United States, who are studying how to spread misinformation online. The team recently identified at least three categories of false or inaccurate information: treatments and ways to prevent infection, the nature of the virus and the alleged laboratory origin of the virus. False treatments and methods of prevention have been the most popular topics for misinformation worldwide[17]. Some examples include:

- ***False health tips***. False advice about health and misinformation continues to be distributed on social networks. Thus, in Turkey, advice such as pure alcohol consumption or the idea that "Turkish genes are immune to the virus" continues to circulate on online platforms.
- ***Rumors of conspiracy theories*.** A huge volume of rumors about conspiracy theories about the "man-made" virus and "miracle cures" has emerged, especially in southeastern Europe. Such content continues to circulate widely in EU Member States.
- ***Origin of the coronavirus***. A ProPublica investigation[18] revealed a network of fake Twitter accounts originating in China that were used to spread misinformation about COVID-19. Thus, in the Chinese intelligence space, there have been attempts to suggest, for example, that it was the US military personnel who brought the virus to Wuhan or that its origin was, in fact, in Italy.

One of the most widespread conspiracy theories related to coronavirus is that 5G technology would spread the virus. "(...) In March and April 2020, small groups of British citizens began to vandalise and in some cases destroy 5G telecommunications masts, based on the spurious belief that they are being used to spread coronavirus. Superficially, the idea that 5G masts might be spreading a biological pathogen seemed so ridiculous to many that early media and government commentary attributed it to 'crazed' and 'crackpot' social media activity"[19]. The European Commission and the World Health Organization have already stressed[20] that there is no link between COVID-19 and 5G technology, and that viruses are not spread via radio waves / cellular networks.

---

[16] World Health Organization, *Novel Coronavirus(2019-nCoV) Situation Report – 13*, 2 February 2020, p.2, URL: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6, accessed on 24.08.2020.

[17] European Commission, Identifying conspiracy theories, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en, accessed on 24.08.2020.

[18] *** "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus", *ProPublica*, URL: https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus, accessed on 24.08.2020.

[19] T. Colley, F. Granelli and J. Althuis, *Disinformation's Societal Impact: Britain, Covid, And Beyond*, volume 8, Spring 2020, p. 107.

[20] *Fighting Disinformation*, European Commission, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_en?fbclid=IwAR0SeWGDV9QMoM8Oegi3EiRJqQY4ZmmhAa7xwlk7NPGv40ICrHTLaf8OEfM#bewareofonlinescams, accessed on 24.08.2020; *Coronavirus disease (COVID-19) advice for the public: Mythbusters*, World Health Organization, URL: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters, accessed on 24.08.2020.

Another widespread myth about coronavirus is that when there is a vaccine against the virus, everyone will be required to be vaccinated, including those who do not want to.

According to a study, „misinformation and rumors regarding COVID-19 are hindering the practice of healthy behaviors (such as handwashing and social distancing) and promoting erroneous practices that increase the spread of the virus and ultimately result in poor physical and mental health outcomes"[21].

Disinformation is also "reducing the legitimacy of new scientific discoveries regarding potential cures or vaccine candidates for this disease. These hoaxes and rumors are also creating a social stigma around COVID-19, which has resulted in reduced compliance with home quarantine and social isolation. Several countries have reported incidents where hundreds of individuals were infected by a single person who visited their mosque/church despite their doctor's advice to remain isolated at home. Such problems are contributing to the suboptimal control of the COVID-19 pandemic across various populations"[22].

The World Health Organization, itself the subject of conspiracies, has also dedicated itself to demystifying the new coronavirus. The WHO shows that drinking alcohol does not protect against infection, the ability to hold your breath for 10 seconds does not prove that someone is not infected and exposure to very high / low temperatures neither cures nor prevents anything.

The Czech Center for Combating Terrorism and Hybrid Threats, which is responsible for monitoring disinformation campaigns with a potential threat to the security of the Czech Republic, considers that information manipulation efforts may be an attempt to exploit the pandemic "in the interests of a large number of potential actors"[23]. Also, the impact of disinformation crosses state borders. A survey conducted by the Moscow School of Economics shows that a quarter of Russia's population believes that the pandemic is not real[24]. And in the US, 30% of the population believe that the virus was most likely created in a laboratory[25], a theory that contradicts all geneticists' studies of the origin of the new coronavirus.

Conclusions

Disinformation doesn't stop at borders, not even with COVID-19. This may have consequences for the stability and security of the EU and its member states. That is why the government supports information exchange about this in a European context, such as through the EU Rapid Alert System. Addressing disinformation is primarily a task of journalism and science, whether or not in collaboration with internet services. Freedom of expression is paramount at all times. However, the government must act when national security, political, social and / or economic stability is at stake. Research is therefore needed to better understand the origins and spread of disinformation, as well as coordinated efforts to disrupt its sources and identify, remove and reduce its spread.

[21] Samia Tasnim, *op.cit*., p.171.
[22] Samia Tasnim, *op.cit*., p.172.
[23] ***, *Coronavirus: An overview of the Main Disinformation Narratives in the Czech Republic*, The Czech Center for Combating Terrorism and Hybrid Threats, URL: https://www.mvcr.cz/cthh/clanek/coronavirus-an-overview-of-the-main-disinformation-narratives-in-the-czech-republic.aspx, accessed on 24.08.2020.
[24] A.N.: Almost quarter of Russians believe coronavirus is fictional, according to new study, *Russia Today*, 28 May 2020, URL: https://www.rt.com/russia/489996-quarter-russians-believe-coronavirus-fictional/, accessed on 23.08.2020.
[25] ***, "Nearly three-in-ten Americans believe COVID-19 was made in a lab", *Pew Research Center*, URL: https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/, accessed on 23.08.2020.

Social media could be used as a diagnostic tool and reference system. Social media should be used to spread reliable information about when to get tested, what to do with the results, and where to get assistance. If a vaccine becomes available, the same platforms could be used to encourage recruitment and address the challenges associated with vaccine hesitation. Social media platforms are well organized and this could be used to direct people to COVID-19 testing resources. For those whose test results were positive for COVID-19, the platform could allow users to inform their contacts about potential exposure and how to follow up the tests.

New approaches are needed to improve the education of health professionals. Social distancing will affect clinical training (e.g. internship in the emergency department) and didactic education (e.g. anatomy laboratory). Social media can be a useful tool to facilitate contact between students and support active learning.

Building a culture of "preparation" is also very important. More than 100 years ago, a global pandemic affected over 500 million people around the world. Today, in the midst of another public health emergency, some lessons from history demonstrate the importance of understanding how information spreads and how individuals interact. Social media integration as an essential tool for preparedness and recovery can influence the response to COVID-19 and future threats to public health. The social stability and protection of public health require active government information with regard to the virus, in which citizens can obtain reliable information about the context and measures surrounding the fight against COVID-19. In some cases, this also requires actively contradicting misleading information.

In conclusion, disinformation powered by conspiracy theories can have possibly serious implications on global public health. Disinformation hampers the mission of public health authorities to get their message across and to give people the right information to stay healthy and safe. In addition, it fuels panic and anxiety, and this can unbalance us mentally. And, obviously, listening to false medical opinions can lead to catastrophic decisions for health and life.

BIBLIOGRAPHY:

1. ***, "Almost quarter of Russians believe coronavirus is fictional, according to new study", Russia Today, 28 May 2020, URL: https://www.rt.com/russia/489996-quarter-russians-believe-coronavirus-fictional/
2. ***, "Coronavirus disease (COVID-19) advice for the public: Mythbusters", *World Health Organization*, URL: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters
3. ***, "Coronavirus Disease 2019 (COVID-19) Situation Report – 13", *World Health Organization*, 2020, Geneva, Switzerland.
4. ***, "Coronavirus: An overview of the Main Disinformation Narratives in the Czech Republic", *The Czech Center for Combating Terrorism and Hybrid Threats*, URL: https://www.mvcr.cz/cthh/clanek/coronavirus-an-overview-of-the-main-disinformation-narratives-in-the-czech-republic.aspx.
5. ***, "Disinformation", Merriam-Webster Dictionary, URL: https://www.merriam-webster.com/dictionary/disinformation
6. ***, "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus", *ProPublica*, URL: https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus
7. ***, "Nearly three-in-ten Americans believe COVID-19 was made in a lab", *Pew Research Center*, URL: https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/

8. ***, "Novel Coronavirus (2019-nCoV) Situation Report – 13", *World Health Organization*, 2 February 2020, p. 2, URL: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6
9. ***, "Study: Distorted Chinese, Russian virus news takes root in West", *Press From*, URL: https://pressfrom.info/us/news/world/-469008-study-distorted-chinese-russian-virus-news-takes-root-in-west.html
10. ***, "The Coronavirus: a Vast Scared Majority around the World – Snap poll in 28 Countries", *Gallup International Association*, March 2020, URL: https://www.gallup-international.com/wp-content/uploads/2020/03/GIA_SnapPoll_2020_COVID_Tables_final .pdf.
11. ***, "Understanding the infodemic and misinformation in the fight against COVID-19", *PAHO*, URL: https://iris.paho.org/bitstream/handle/10665.2/52052/Factsheet-infodemic_eng.pdf? sequence =14
12. ***, *Eeas Special Report Update: Short Assessment of Narratives and Disinformation around the Covid-19 Pandemic*, EU vs. Disinfo, April 01, 2020, URL: https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic/
13. ***, *EEAS Special Report: Disinformation on the Coronavirus – Short Assessment of the Information Environment*, March 19, 2020, URL: https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/
14. ***, *Fighting Disinformation*, European Commission, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fightingdisinformation_en?fbclid=IwAR0Se WGDV9QMoM8Oegi3EiRJqQY4ZmmhAa7xwlk7NPGv40ICrHTLaf8OEfM#bewareofonline_scams
15. ***, *Identifying conspiracy theories*, European Commission, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en
16. COLLEY, T.; GRANELLI, F., ALTHUIS, J., "Disinformation's Societal Impact: Britain, Covid, And Beyond", volume 8, Spring 2020.
17. REBELLO, Katarina; SCHWIETER, Christian; SCHLIEBS, Marcel, et. al., *Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users. Understanding Chinese, Iranian, Russian and Turkish Outlets, Data Memo 2020*, Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk, URL: URL: https://comprop.oii.ox.ac.uk/research/covid19-french-german-spanish
18. TASNIM, Samia; HOSSAIN, Md Mahbub, MAZUMDER, Haimonty, "Impact of Rumors and Misinformation on COVID-19 in Social Media", *Journal of Preventive Medicine & Public Health*, 2020 May, 53(3): 171–174, URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280809/

THE DIGITAL SCARS LEFT BY THE COVID-19 PANDEMIC

Ion-Alexandru MANOLIU
Technology Analyst, Senior Software Developer, Directorate-General for Research and Innovation, European Commission, Cybersecurity Researcher, Center for Conflict Prevention and Early Warning, Bucharest, Romania. E-mail: office@mdigital-group.com/office@cloudast-tech.com

Abstract*: Correlating the economic prosperity of a nation with the quality of its cyber infrastructure is not a game of chance. Improving cybersecurity in society, the industrial system and public administration will become increasingly stringent. The lack of security professionals makes companies, organizations and social services more vulnerable. As the global health emergency from Covid-19 taught us, coordination from the top of the chain of command is important. Whether it is to minimize intrusions, data loss or the spread of malware, the collaboration of all state institutions and private sector is essential. Developing new capabilities and tools to improve the cyber security of the country system is a challenge of the utmost importance for the growth and well-being and security of all. Cyber security education in the conscious use of the network therefore will play a central role in both the defense and development of a country.*

Keywords*: cybersecurity; digital education; infrastructure; defense; health-emergency.*

Introduction

Since the beginning of this year, one of the most debated topics is the COVID-19 pandemic, which has forced the whole society to take measures of distance or physical isolation, which has led to a rapid increase in the use of digital technologies in all areas. The rapid rise in data traffic, time spent online, and access to personal use, smart working, remote working, educational processes, business interactions, or simple social media accesses or interactions have exponentially increased exposure to cyber-attacks in turn, it exponentially multiplied the risks of increasingly new scenarios and opportunities for online crime.

The increasing use of technological tools, the growing periods of time spent online, the growing number of users, the growing number of procedures, online operations and applications for every private or professional need have created a Babylon tower of digital interactions and risks of which the vast majority are not even aware.

The ever-expanding field of cybersecurity is a field of increasingly important risks in which everyone is involved, from state and private entities that create the rules and legal framework to the occasional user. On this field of confrontation, those who capitalize on points, entities that are not always benevolent, very often with criminal intentions and plans and at any time on the hunt for information, data, benefits, advantages and personal gains are emerging on the surface. In this type of ecosystem, the dangers are not always perceived to be of real importance.

Cyberspace is the most complex thing that man has ever built: on one hand, a union of thousands of networks that make it difficult even to have a snapshot of who is connected to it, on the other, stratification of software programs and protocols developed in the last 40 years.

This complexity generates vulnerabilities (software errors, incorrect configurations

and weaknesses in the protocols) which are exploited by cyber criminals to steal data or cause damage.

In an increasingly digitalized world, cyber-attacks raise alarm in the population, cause serious damage to the economy and endanger the same safety of citizens when they hit distribution networks of essential services such as health, energy, transport, worth to say the critical infrastructures of modern society. In Europe, entire sectors, such as mechanics, shipbuilding, tourism, agri-food and transport, could undergo heavy reductions in turnover due to attacks perpetrated in cyberspace by sovereign states or by competitors.

A successful cyber-attack could represent a moment of no return for the credibility of a company, the development of its business and the ability to sell products in a regime of healthy competition. Equally, a successful cyber-attack could destabilize the stock market by plunging entire countries into chaos, or blocking gas supplies in the winter or managing the municipal waste cycle.

Many times, the damage of cyber-attacks depends on a weak link and often this is the human factor. Man, and his digital footprint is now a part of cyberspace and represents the most important and unpredictable vulnerability of this macrosystem. A wrong click can in some cases destroy any technological defense line of an institution, an organization, a country. This are the people who get "caught" by a phishing campaign, who use the name of the cat or their spouse as a password, who use the same smartphone to let their children play and to access the corporate network. They are the first to open doors to criminals to their organizations' sites, networks and databases, with dangerous and unpredictable effects.

A country that does not put cybersecurity at the center of its digital transformation policies is therefore a country that seriously jeopardizes its economic prosperity, security and independence.

1. A cyber-pandemic synergy

The major dangers during the pandemic in the first part of this year were intensely experienced at the individual level. Companies have raised the level of control to deal with new types of attacks, particularly automated. Attacks designed to penetrate security systems and cause significant damage to companies' structures identified as potential targets or victims at high risk of penetration.

Most criminal attacks have the primary purpose of access and then destruction of antivirus and firewall systems to prepare the ground for major fraud or a bigger action. In order to deal with this type of attacks, it is necessary to identify in time, from the first signs of the attack triggered in order to act quickly and effectively to protect the integrity of the computer and infrastructure systems. The most effective defense tools and weapons to be implemented are those based on technologies capable of evolving through machine learning because they use the means and principles of artificial intelligence systems superior to human reaction capabilities.

Particular attention should be paid to large companies and organizations that are already in the spotlight for cybercrime which interest is strongly economic. Most of the attacks strategy used is built on continuously evolving ransomware time tools and are able to take advantage of organizational, computer and human vulnerabilities to penetrate societal processes and procedures with devastating effects. Defending against ransomware attacks should become a priority but this can only be done by activating the necessary prevention systems that include continuous and proactive monitoring of attacks and events that can signal potential attacks in training or preparation. This type of attack identification cannot be done with traditional defense tools.

With the onset of the pandemic, another area of vulnerability in the fight against cybercrime has emerged, namely that of misinformation. Those who were more careful and cautious about cyber-attacks are witnessing the proliferation of fake news, increasingly widespread conspiracy theories and false truths spreading on the battlefield of misinformation and manipulation. In this vitiated environment, there are those who fall victim to false information, in which they participate consciously or not and those who are already victims of misinformation and who in turn propagate the false truth.

The increasing danger of these types of cybercrime specific activities has been facilitated by the rapid and continuous growth of Internet activities, increasingly widespread and use of technological platforms, increasingly sought-after search engines, and exponentially growing social media and messaging platforms. Platforms such as Instagram, Twitter, Facebook, Dating, and daily activities like shopping are constantly growing and data traffic includes more and more domains and types of information vectors.

The objective of these types of cybercrime is simple to observe and is defined by the intention to manipulate the individual's perceptions in order to influence and direct him to choices, creating preferences and needs decided by those who manage this vast field of cybercrime. Even if it seems that the objectives of cybercrime are predominantly political, the economic and pecuniary objectives are equally important when the targets are large companies, brands, organizations, production chains, business, trade or numerous social groups. The danger of these attacks comes with the near impossibility of avoiding them, doubled by the lack of adequate legislation for combating cybercrime.

In most structures under cyber-attacks, the prevailing defense reaction is mostly technological. What is missing instead is the cultural approach to correct and obtain relevant information based on collaboration with partners with the same approach and with viable and reliable principles of organizational culture.

Also, the cyber and digital security of public administrations which, although operating with a huge amount of sensitive data and personal information, are not protected to the extent of the devastating effects of targeted cyber-attacks. The university field [1]is the most targeted by cyber-attacks, followed by Ministries, County Councils, City Halls, Hospitals and educational structures [2]across USA and UK.

2. Health, one of the most vulnerable sectors by cyberthreats during COVID-19

The World Health Organization reported in the first half of 2020 since the beginning of the Covid-19 pandemic a staggering increase in cyber-attacks compared to the same period in 2019. The attacks targeted agency staff involved in the state of emergency generated by the Covid-19. To protect computer systems, many of them were moved to more secure operating systems. A significant increase was observed in the use of e-mail platforms endangered by phishing and scamming attacks.

WHO recommended to its staff to use official sources to obtain real information[3]. Emails containing malware have been disseminated to create the conditions for fraudulent

[1] Jamie Grierson, Hannah Devlin, "Hostile states trying to steal coronavirus research, says UK agency", *The Guardian*, URL: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency, accessed on 14-06-2020.

[2] ***, "COVID-19 Cybercrime Analysis report August", *Interpol*, URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, accessed on 08-08-2020.

[3] ***, "WHO reports fivefold increase in cyber attacks, urges vigilance", *World Health Organization*, URL: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance, accessed on 03-05-2020.

scams by stealing users' personal data generated by requesting data under the pretext of protection against the risk of a virus caused by installing harmful files or providing bank data from personal desk computers directly to cybercriminals.

Through deceptive emails such as coming from WHO, the attackers requested the installation of a file that actually contained a Trickbot[4], malware capable of stealing documents, and access passwords from users' computers. Most of the time, the Trickbot is accompanied by a Ryuk[5] ransomware that locks the computer by encrypting the files and requesting ransoms to unlock them.

Cyber-attacks in the context of coronavirus pandemic were hidden in links that pointed to files with .pdf coronavirus defense instructions but were actually harmful executable files. The same kind of attacks came through e-mail as from some banks that invited customers to check if there was any data access precisely for the dangers and computer attacks caused by the coronavirus alarm. Fear, which is normal in this case, caused users to open attached files which, once accessed, caused major damage to the computers and users.

IBM X-Force and Kaspersky reported the existence of computer viruses that exploited the fear of coronavirus infection[6]. The Emotet[7] virus, which targets banking data, has proven to be extremely capable of finding banking data in attacked computers, which were then used to hijack users' accounts.

The United Kingdom, the USA and Canada are coordinating against computer attacks of Russian origin that target even the computer platforms used to produce anti-Covid-19 vaccines. Attacks managed by Russian intelligence services against pharmaceutical groups engaged in vaccine production have been discovered[8].

The National Cyber Security Center (NCSC) discovered a group of hackers called APT29 and also known as Cozy Bear behind this type of attack and confirmation of the existence of these attacks came from the NSA and the Canadian intelligence authorities[9].

However, the Russian side through the spokesman of the President of the Russian Federation stated that this information is not real and that Russia is not involved in this type of cyber-attacks.

The Covid-19 pandemic highlighted the cyber fragility of public structures and private companies in the healthcare field either through the negative effects suffered or through the absence of appropriate international legal norms.

---

[4] ***, "TrickBot Attack Exploits COVID-19 Fears with DocuSign-Themed Ploy", *Threat Post*, URL: https://threatpost.com/trickbot-attack-covid-19docusign-themed-malw/155391/, accessed on 06-07-2020.

[5] ***, "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware", *Crowd Strike*, URL: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/, accessed on 14-02-2020.

[6] Alice Baker, "Criminal hackers exploit fear of coronavirus to spread malware", *IT Governance*, URL: https://www.itgovernance.eu/blog/en/criminal-hackers-exploit-fear-of-coronavirus-to-spread-malware, accessed on 04-06-2020.

[7] Limor Kessem, Ashkan Vila, "Emotet Activity Rises as It Uses Coronavirus Scare to Infect Targets in Japan", *Security Intelligence*, URL: https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/, accessed on 12-06-2020.

[8] Zachary Cohen, Luke McGee and Alex Marquardt, "UK, US and Canada allege Russian cyberattacks on Covid-19 research centers", *CNN*, URL: https://edition.cnn.com/2020/07/16/politics/russia-cyberattack-covid-vaccine-research/index.html, accessed on 17-07-2020.

[9] ***, "Weekly Threat Report 17th July 2020", *NCSC*, URL: https://www.ncsc.gov.uk/report/weekly-threat-report-17th-july-2020, accessed on 24-07-2020.

Europol has reported[10] that in the wake of the Covid-19 attacks on healthcare facilities, hospitals, national health systems and biotechnology companies by cybercriminals have increased exponentially worldwide.

The health sector remains a gold mine with sensitive data at the disposal of cyber attackers precisely because this field is not prepared to defend itself effectively against this type of targeted attacks. Only in March 2020 did the University Hospital in Brno[11], Czech Republic and the US Health Agency[12] fall victim to cyber-attacks and endanger the health of patients, surgeries and timely conduct of COVID-19 tests. Distributed Denial of Service (DDoS) attacks have blocked the servers of those healthcare facilities through millions of fake access attempts.

As soon as the first attacks were signaled, Interpol launched a global alarm on the blocking of cyber-attacks on hospital structures and medical staff, which led to demanded ransom payments in order to unblock the vital medical files or computer mechanisms attacked.

In the US in mid-March this year, there was a targeted attack on the Department of Health & Human Services[13] aimed at undermining the state's efforts to respond as effectively as possible to the alarming increase in the number of pandemic victims. While all attention was focused on saving lives in the health system, the number of cyberattacks has increased alarmingly.

From a cybernetic point of view, the current coronavirus pandemic, which has brought the economies and health systems of many countries around the world to their knees, can be characterized as one of the most aggravating and persistent wave of cyberattacks ever experienced, essentially from the perspective of fake news, privacy and data breaches.

The size of the cyber-attacks, the multitude of technologies involved, the multitude of targeted subjects, the size of the amounts demanded as ransom and the economic damage suffered reveal a truth that is hard to accept: almost all health information systems in most of the states are extremely fragile and necessary at a time with accentuated crisis in which human lives are at stake and under the attack of an invisible but extremely dangerous enemy.

One of the main causes of the lack of adequate responses to this type of cyber-attack remains the lack of a unified international legal framework and unified procedures that can create an effective defense system.

International humanitarian law can be applied only in the case of cyber-attacks against hospital structures, only in case of armed conflict. In the absence of these exceptional conditions, cyberspace transcends the national boundaries between the state of war and the state of peace on which this field of law is traditionally based. In peacetime, there are no legal rules on cyber-attacks in cyberspace.

---

[10] ***, "Catching The Virus Cybercrime, Disinformation And The Covid-19 Pandemic", *Europol*, URL: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, accessed on 10-06-2020.

[11] ***, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak", *ZDNET*, URL: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/, accessed on 14-03-2020.

[12] Shira Stein, Jennifer Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak", *Bloomberg*, URL: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response, accessed on 20-03-2020.

[13] Haley Samsel, "Cyber Attack Hits Department of Health and Human Services Amid Government Coronavirus Response", *Security Today*, URL: https://securitytoday.com/articles/2020/03/18/cyber-attack-hits-department-of-health-and-human-services-amid-government-coronavirus-response.aspx, accessed on 08-07-2020.

Cyber-attacks that endanger the health sector of a state could, in theory, be interpreted as violations of the sovereignty of that state. However, no clear conclusion has been reached on the obligation to respect state sovereignty in cyberspace.

Among the companies established in the field of data protection and cybersecurity is the Swiss group Acronis, which reports a steady increase in ransomware attacks in Europe [14] targeting state and private healthcare systems and their medical staff. In an attempt to raise the level of cyber security and defense of its systems, they recommend digitizing the processes of data transmission and use it even if through this technological leap they become of interest to attackers. For a better defense of companies and organizations against ransomware attacks, Acronis recommends defining and implementing anti-phishing strategies based on the training of operating personnel so that they can easily recognize potentially dangerous emails and sites. Wherever possible, two-step authentication and the use of complex passwords are required. Even turning public websites into static websites can help defend against ransomware attacks by using technologies based on artificial intelligence.

Among the groups on the front lines of defense against cyberattacks is Kaspersky, who considers [15] health facilities to be among the most vulnerable targets in this pandemic-marked period. Switching to the home-working method did not reduce the danger created by cyber-attacks but on the contrary, the size and multiplication and diversity of forms used increased.

To support the fight against cyber-attacks, the Kaspersky group offered their security solutions free of charge for six months.

Attacks on health and hospital facilities in this period marked by the Covid-19 crisis should be considered terrorist attacks because attackers and victims of attacks can be assimilated to the field of terrorism, which, interpreted in a virtual way, presents itself as more controversial and obscure than traditional terrorism.

At the terminological level, the concept of cyber terrorism is at least porous due to the absence of an international legal framework that inevitably leads to debate around it and its actual existence. In addition, some find it difficult to recognize evidence of cyberterrorism, while others believe that some groups routinely use the Internet in terrorist ways.

One point that can be considered, however, is that our society's growing dependence on computer and telematics technology continues to generate new forms of vulnerability, giving terrorist groups the opportunity to have access to targets that were completely inaccessible until a few years ago. such as national defense systems, control systems and transport of people and goods (air, rail, naval, road), management structures of energy sources such as dams or nuclear power plants, health systems, economic and financial circuits, etc. The technological advancement of each country, therefore, can only correspond to a greater vulnerability of the it's critical infrastructure.

A particularly serious warning signal is the fact that police structures have discovered that on a global scale the cyber-computer attacks during the pandemic increased by 600% compared to last year[16].

Cyber-attacks targeted a wide range of interests from state initiatives, industrial espionage or political or ideological activism. Another preferred area for cyber attackers was

[14] Alexander Ivanyuk, "As COVID-19 Spreads, So Do Ransomware and Cryptomining Attacks", *Acronis*, URL: https://www.acronis.com/en-us/blog/posts/covid-19-spreads-so-do-ransomware-and-cryptomining-attacks, accessed on 20-04-2020.

[15] Nikolay Pankov, "Protecting health care", *Kaspersky Daily Blog*, URL: https://www.kaspersky.com/blog/ protecting-healthcare- organizations/34269/, accessed on 25-03-2020.

[16] ***, "Understanding and dealing with phishing during the covid-19 pandemic", *Enisa*, URL: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic, accessed on 12-06-2020.

drugstores, fundraising actions for Covid-19 victims, or interest and curiosity in providing information on pandemic spread maps.

3. Personal data theft and economic fraud

From January to April 2020, there was an increase of over 50% in the number of attacks that had as a defining element the remote work, smart working and online distance teaching and educational activities[17]. There was also a spectacular increase in connections and their duration during the lockdown period, especially when the most requested arguments and areas of interest were the state of emergency caused by Covid-19. During that time, various illegal or uncertain sites exploited terms and phrases such as Corona and/or Antivirus and distributed files with malicious software on the computers of less trained users in the field of computer security.

Reasons that have allowed or even facilitated the spread of these attacks include the lack of a digital culture in line with current challenges as well as the low level of protection of state and private organizations operating with sensitive data volumes. The effects of the attacks were mostly the theft of personal data from penetrated computers and the violation of privacy. In most of cases there were e-mails with malicious attachments, misleading offers of money loans, shopping on unverified sites, or malware that has exploited the fear of coronavirus or the curiosity of users without a minimal computer culture. Spyware under false identity and use with various names such as *CovidLock*, *Corona Antivirus* or *Covid-19-Antivirus* allowed attackers to enter users' computers to spy on their content, steal sensitive data or create conditions for further attacks[18]. One element that contributed major to reducing the efficiency of computer security systems was the massive use of smart working and the use of personal terminals increasingly required by smart-tv, smartphones, cameras, printers connected to home networks or home automation that are were not upgraded in time, generated significant risks for employees and employers.

The year 2020 should have been a turning point and the launch of a decade of technological development, but unfortunately it proved to be a very difficult year starting with all the corollary of inconveniences that Covid-19 has brought so far for health, work and global economy or societal development.

An important cause of the increased exposure to cyber-attacks and vulnerability of law enforcement systems was the increase in the share of domestic work outside the normal perimeters in which companies/organizations operated. This decrease in cyber defense capacity has resulted in an opportunity not to be overlooked by cybercrime.

Unfortunately, this whole period has brought with it an alarming increase of cyber-attacks of which, between 200 and 600% of them involved fraud and damage in all digital areas. By taking advantage of the cracks and weaknesses of computer security systems in the pandemic-marked period, cybercriminals have made increasingly sophisticated attempts to access users' sensitive data and information through social engineering, e-mail phishing or creating fake websites.

Classic authentication systems based on passwords and PINs have demonstrated their limits in terms of the exponential increase to risks due to new technologies used by

[17] Mark Scott, Laurens Cerulus, Janosch Delcker, "Coronavirus is forcing people to work from home. Will it break the internet?", *Politico*, URL: https://www.politico.eu/article/coronavirus-covid19-internet-data-work-home-mobile-internet/, accessed on 17-03-2020.

[18] ***, "Pandemic Profiteering: How Criminals Exploit the Covid-19 Crisis Report", *EUROPOL*, URL: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis, accessed on 27-03-2020.

cybercriminals. Exactly at times like this when the society is going through the threat of the pandemic, it is becoming increasingly clear how hackers target the most vulnerable victims for stealing sensitive information through e-mail, SMS or direct personal communications.

In the absence of adequate protection systems capable of detecting cyber-attacks, attackers may take possession of user accounts, private or state customer funds. Not even the OTP (One Time Password) system via SMS can provide protection against cyber-attacks. A skilled hacker can access enough data about a potential victim to be able to access his telephone account for intercepting SMS with OTP that are sent by banking service providers using SS7 techniques[19].

In 2019 alone, cyber-attacks cost the global economy more than $5 billion and the average damage to victims of attacks amounted to more than $ 2,000 per person just because of errors or stolen passwords.

An increase in the efficiency of authentication systems can be generated by the use of biometric data[20] to enable sensitive service providers to more effectively protect against cyber-attacks and to ensure the security of their customers and employees. Also, the use of a human voice with a personal stamp or a fingerprint doubled by the use of sophisticated algorithms can ensure a high degree of protection.

A higher level of protection can be ensured by the behavioral biometrics that are based on the way the characters are typed, or by the way the keys are touched when the screen is touched can give enough identification elements of the real user. The combined use of several multifactorial authentication technologies, end-to-end encryption in public key IT infrastructures together with the use of biometric data can be a shield against cyber fraud.

With the emergence and global spread of the Coronavirus crisis, there has been a radical change in the interest of users, operators and cybercriminals mostly in information, news and statistics to which hundreds of millions of people have had access in an extremely unsafe time. With the same speed, the means and vectors of misinformation, manipulation and fake news spread.

Such an opportunity could not be missed by cybercriminals who knew how to exploit and deceive potential victims driven by curiosity, thirst for hot topics or a desire to stand out in any way. This combination of declining cyber protection doubled by increasingly sophisticated attacks and adapted to the targets chosen by hackers has resulted in a huge volume of privacy violations, theft of personal, health, banking or financial data, computer system blockages in almost all areas and huge sums of money stolen from the victims of the attacks.

In addition to these damages, there were restrictions on movement and social distancing, lockdown, stopping the entire economic sectors of production and services, the continuous increase in the number of infections and the spiking levels of fear and panic among society.

In most of the cases, IT security teams have been overwhelmed by the actual spread or dislocation of employees, outside the premises, further exacerbated by the use of home computers, terminals or private network providers totally surpassed by the exponentially increased volume and data traffic in the first days of the emergency state.

[19] Stefan Topuzov, "Phone hacking through ss7 is frighteningly easy and effective", *Secure Group*, URL: https://blog.securegroup.com/phone-hacking-through-ss7-is-frighteningly-easy-and-effective, accessed on 12-06-2020.

[20] ***, "Biometric authentication", *Science Direct*, URL: https://www.sciencedirect.com/topics/computer-science/biometric-authentication, accessed on 06-08-2020.

4. Software surveillance, balancing security and democracy during COVID-19

Around the world, several states are currently adopting software-tools that use personal data to manage the Covid-19 emergency. Some of these are statistical analysis, mainly use the aggregated and anonymized data of the telephone operators to map the concentration of people in the various areas.

In this regard, even Google, using the information collected with the history of the positions of its maps, has provided aggregate data on travel in Europe.

In the United States this type of aggregate analysis on the movements of people was also made by a startup, Unacast[21], which used the location data obtained from a series of apps for shopping, gaming etc.

Some tools used by some states are instead self-assessment and initial triage; in practice they are apps that allow people to have a first assessment and contact on their health without clogging the emergency lines, and have been adopted for example in Spain[22].

Then there are those who intend to apply the rules on quarantine and lockdown, such as the Home Quarantine app of Poland [23] which requires you to send regular geolocated selfies following a message at which users have only twenty minutes to respond to a photo request.

In this context, in which there is a strong temptation to resort to solutions and approaches derived from intelligence, anti-terrorism, surveillance and the criminal system, and in which haste risks favoring ready-to-use solutions, it must be remembered that COVID-19 is not a technological problem, and that the countries often cited as models - Singapore, South Korea etc. also took other measures and started from a different level of preparation and intervention. Therefore, there is no ideal and identical solution for everyone.

Testing, contact tracing and quarantine are probably the three ingredients for success in the fight against coronavirus but the contexts are different and the technological solutions adopted can give different results. So, there is no need to rush to implement mass digital surveillance tools, and civil society can and must contribute to the debate on which alternatives to embrace. In fact, the solutions to combat the virus and protect privacy are not mutually exclusive, some projects - like the Algorithm Watch [24]- go in this direction. Ultimately, every proposal adopted must be compatible with democracy.

The measures adopted - including any technologies for tracking people, their state of health, their movements and their contacts if they are infected - must be able to answer a series of questions. There is a strong risk that the result obtained as can impact the civil society different ways, and act as limitations to personal freedoms and intrusions into private life.\ Above all, that tracking and surveillance approach drags behind a propensity for secrecy, typical of those involved in national security, as well as the idea that data and

[21] John Scott Lewinski, "Unacast Grades The 'States' Of Social Distancing With COVID-19 Report Card", *Forbes*, URL: https://www.forbes.com/sites/johnscottlewinski/2020/05/07/unacast-grades-the-states-of-social-distancing-with-covid-19-report-card/, accessed on 03-08-2020.

[22] Guillermo Vega, "Spain launches first phase of coronavirus-tracking app", *EL Pais*, URL: https://english.elpais.com/society/2020-06-29/spain-launches-first-phase-of-coronavirus-tracking-app.html, accessed on 06-08-2020.

[23] Caitlin O'kane, "Poland is making quarantined citizens use a selfie app to prove they're staying inside", *CBS News*, URL: https://www.cbsnews.com/news/coronavirus-update-poland-quarantine-app-asks-selfies-to-prove-isolation-social-distancing-police-patients/

[24] ***, "Automated decision-making systems and the fight against COVID-19 – our position", *Algorithm Watch*, URL: https://algorithmwatch.org/en/our-position-on-adms-and-the-fight-against-covid19/, accessed on 08-07-2020.

procedures must be kept hidden because the enemy could exploit that knowledge to defend himself.

Applying this kind of paraphernalia, technical and mental, to the health emergency also means carrying an approach (often present in the management of public law and order and intelligence) for which citizens are seen as possible suspects, rather than as responsible subjects capable of collaboration, endowed with rights and ultimately protagonists of the fight against the epidemic.

5. A need for a global cyber defense education: final thoughts

Developing new digital skills and new tools to improve the cyber security of a country infrastructure system represents a challenge of the utmost importance for growth and for the well-being and safety of all. Cybersecurity in this perspective must be based on education in the conscious use of the network, and in the acquisition of a series of knowledge.

More than anything, it is important to distinguish ourselves from the machines, learning to do things that make us human, how to expand data and information analysis skills critically, evaluating the sources and their reliability, understanding the meaning and implications of involuntary sharing or creating false information, the ability to improve the attitude to face complex problems and the knowledge of the principles that allow us to connect this knowledge and make sense of it.

Emergency situations offer the opportunity to accelerate experimentation with innovative solutions and develop better strategies based on experience.

It is a fact that even in a situation of extreme difficulty, the need to react is opening us up to possibilities and tools that were previously little or not used at all.

Technology is helping us out and at the same time, more and more people are experiencing the importance of protecting data that travels on the network. As technology progresses, it will change the type of cyber skills required of humans. If we are ready to take this opportunity, we will see an improvement that will help ensure greater protection of citizens' privacy and at the same time of critical infrastructures.

Investing in cyber security training provides a unique answer to many of a country's problems and becomes indispensable in the context of the progressive digitalization. Training the new generations will trigger a virtuous process in which the managerial class and technicians of the future will have the skills, cultural background and operational skills necessary to confront the technological and scientific challenges that will change our lives in the coming decades, developing the initiatives necessary to face the continuous changes and the related risks that await us in the future.

Scientific research is also essential to address the challenges that cybercrime poses to the digital society. The challenges concern both scientific research and technological innovation. In many cases, in addition to obtaining theoretical results, it is necessary to create prototype systems aimed at a more rapid industrialization of solutions. Given the diversity of objectives and skills needed to face these challenges, a strong synergy is needed between the world of scientific/military research and industrial/private.

In particular, private companies will play a fundamental role - within an integrated system - in the subsequent prototyping and industrialization of the needed solutions, innovative approaches defined on the basis of scenarios and requirements identified in a collaborative way.

All this will allow for a timely and effective technology transfer. Finally, an important role should be assigned to the Government and the institutions in terms of defining the

necessary regulatory frameworks and implementing funding programs to address the emerging digital challenges.

A global effort is needed to defend our economies from accelerating threats. Cybersecurity training and education are and will be an important part of this effort.

BIBLIOGRAPHY:

1. ***, "Automated decision-making systems and the fight against COVID-19 – our position", *Algorithm Watch*, URL: https://algorithmwatch.org/en/our-position-on-adms-and-the-fight-against-covid19/
2. ***, "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware", *Crowd Strike*, URL: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
3. ***, "Biometric authentication", *Science Direct*, URL: https://www.sciencedirect.com/topics/computer-science/biometric-authentication
4. ***, "Catching The Virus Cybercrime, Disinformation And The Covid-19 Pandemic", *Europol*, URL: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, accessed on 10-06-2020.
5. ***, "COVID-19 Cybercrime Analysis report August", *Interpol*, URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
6. ***, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak", *ZDNET*, URL: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/, accessed on 14-03-2020.
7. ***, "Pandemic Profiteering: How Criminals Exploit the Covid-19 Crisis Report", *EUROPOL*, URL: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis
8. ***, "TrickBot Attack Exploits COVID-19 Fears with DocuSign-Themed Ploy", *Threat Post*, URL: https://threatpost.com/trickbot-attack-covid-19docusign-themed-malw/155391/
9. ***, "Understanding and dealing with phishing during the covid-19 pandemic", *Enisa*, URL: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic
10. ***, "Weekly Threat Report 17th July 2020", *NCSC*, URL: https://www.ncsc.gov.uk/report/weekly-threat-report-17th-july-2020, accessed on 24-07-2020.
11. ***, "WHO reports fivefold increase in cyber attacks, urges vigilance", *World Health Organization*, URL: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
12. BAKER, Alice, "Criminal hackers exploit fear of coronavirus to spread malware", *IT Governance*, URL: https://www.itgovernance.eu/blog/en/criminal-hackers-exploit-fear-of-coronavirus-to-spread-malware
13. COHEN, Zachary; MCGEE, Luke, and MARQUARDT, Alex "UK, US and Canada allege Russian cyberattacks on Covid-19 research centers", *CNN*, URL: https://edition.cnn.com/2020/07/16/politics/russia-cyberattack-covid-vaccine-research/index.html
14. GRIERSON, Jamie; DEVLIN, Hannah, "Hostile states trying to steal coronavirus research, says UK agency", *The Guardian*, URL: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency
15. IVANYUK, Alexander, "As COVID-19 Spreads, So Do Ransomware and Cryptomining Attacks", *Acronis*, URL: https://www.acronis.com/en-us/blog/posts/covid-19-spreads-so-do-ransomware-and-cryptomining-attacks
16. KESSEM, Limor; VILA, Ashkan, "Emotet Activity Rises as It Uses Coronavirus Scare to Infect Targets in Japan", *Security Intelligence*, URL: https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/

17. LEWINSKI, John Scott, "Unacast Grades The 'States' Of Social Distancing With COVID-19 Report Card", *Forbes*, URL: https://www.forbes.com/sites/johnscottlewinski/2020/05/07/unacast-grades-the-states-of-social-distancing-with-covid-19-report-card/
18. O'KANE, Caitlin, "Poland is making quarantined citizens use a selfie app to prove they're staying inside", *CBS News*, URL: https://www.cbsnews.com/news/coronavirus-update-poland-quarantine-app-asks-selfies-to-prove-isolation-social-distancing-police-patients/
19. PANKOV, Nikolay, "Protecting health care", *Kaspersky Daily Blog*, URL: https://www.kaspersky.com/blog/protecting-healthcare-organizations/34269/
20. SAMSEL, Haley, "Cyber Attack Hits Department of Health and Human Services Amid Government Coronavirus Response", *Security Today*, URL: https://securitytoday.com/articles/2020/03/18/cyber-attack-hits-department-of-health-and-human-services-amid-government-coronavirus-response.aspx
21. SCOTT, Mark; CERULUS, Laurens; DELCKER, Janosch, "Coronavirus is forcing people to work from home. Will it break the internet?", *Politico*, URL: https://www.politico.eu/article/coronavirus-covid19-internet-data-work-home-mobile-internet/
22. STEIN, Shira; JACOBS, Jennifer, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak", *Bloomberg*, URL: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
23. TOPUZOV, Stefan, "Phone hacking through ss7 is frighteningly easy and effective", *Secure Group*, URL: https://blog.securegroup.com/phone-hacking-through-ss7-is-frighteningly-easy-and-effective
24. VEGA, Guillermo "Spain launches first phase of coronavirus-tracking app", *EL Pais*, URL: https://english.elpais.com/society/2020-06-29/spain-launches-first-phase-of-coronavirus-tracking-app.html

THE COMMON EUROPEAN SECURITY UNDER THE CORONA VIRUS PANDEMIC MASK

Bogdan-Cezar CHIOSEAUA, Ph.D.
LTC Lecturer, "Henri Coandă" Air Force Academy, Braşov, Romania.
E-mail: chiobogdan@yahoo.com

Abstract: *„A safer Europe in a better world" were the words that one could hear in December 2003 at the General Council of the European Union, when the "European Security Strategy" was adopted. It represented a historic moment in which clear targets were set for ensuring security, common threats were identified and principles were promoted in order to give the European Union the status of regional and global "anchor of stability". Five years later, at the presentation of the first report regarding the strategy implementation, the heads of state and government reached a common conclusion, that the world is in a continuous, accelerated and varied change, and ensuring the security in such environment becomes a challenge, a desideratum for which all member countries must contribute. Today, the world is neither better nor safer. An unexpected blow, the Corona virus pandemic has been applied to the political, economic and military interests that are shaking the foundations of the "European Union Pantheon", and its effects are felt in all countries, regardless of their level of development or contribution to the European Union budget.*

Keywords: *Common security; European Union; strategy; interests; pandemic; cooperation.*

Introduction

After 1945, the post-war european countries could hardly recover from the trials they had been subjected to by the largest and most complex world conflagration ever encountered.

The United States give a helping hand and launch a European reconstruction plan, designed by the State Secretary George Marshall, which aims to provide financial assistance worth about $ 13 billion to 16 Western European countries. The plan brings with it the objectives of US foreign policy, objectives aimed at infiltrating the influences of American capitalism, while blocking the rise of the communist current already propagated and implemented by the Soviet Union in Central and Eastern European states.

The Marshall Plan brings revives the industries and economic systems that are on the verge of collapse, and, in addition to its main courses of action (infusion of funds and economic assistance), it manages to achieve what will later shape the idea of forming the European Union - an economic and political cooperation between two of the strongest states, France and Germany, as well as between the states of Europe, still untouched by the scourge of communism. On May 9th, 1950, the declaration of French Foreign Minister, George Schuman, did nothing but authenticate and strengthen the Franco-German economic and political relationship and lay the foundation stone of the future European Union, an alliance that would bring together most European countries, under ideals and values that put first the human rights, freedom, democracy and law.

The values of the European Union are still appreciated and promoted among member countries. To ensure a future "EU alliance", they are built on clear objectives such as peace and freedom, European values, technical and scientific progress, respect for cultural diversity,

solidarity and combating discrimination, creating an economic and monetary union, establishing a competitive market economy and ensuring security and justice without internal restrictions or constraints. These values cannot be defended, and set goals can only be achieved if they operate in a safe and stable security environment. Thus, the European security environment is given special importance, and the 1993 Treaty on European Union, the Common Foreign and Security Policy (CFSP) is given the role of a pillar of the European Union, along with other two, the European Communities and police and judicial cooperation in criminal matters[1].

Today, the European Union and the rest of the world are trying to deal with a unique threat, the Corona virus pandemic, a challenge for all medical systems and an issue whose international evolution is hard to predict. Ensuring the security of citizens requires the adoption of a strategy that will set in motion all mechanisms of collaboration and cooperation - there is a need for „a common vision and unitary actions"[2]. There is also a need for a modern Global Strategy for the European Union's Foreign and Security Policy defining an image of Europe as a „guarantor of security"[3]. But can a European security strategy, which foresees current and future risks and threats, act in an organized way to neutralize them? How does the Corona virus pandemic endanger the security and safety of European citizens? These statements and questions are the ones to which we will try to find answers and justified arguments.

1.The Global Strategy for the European Union's Foreign and Security Policy

Europe has been and still is the cradle of culture and civilization around the world, it is the place where the most important works were conceived and some of the most important inventions were born with significant implications on world culture and economy.

The foundation of the European Union is, in fact, an economic, political and military pact, through which member countries provide their assistance whenever needed and, at the same time, it represents an international system focused on rules and laws based on European citizens and principles such as peace, freedom, prosperity, security, permanent dialogue, solidarity and consensus. Since its establishment, the European Union has faced many situations, crises, incidents that have been generated from two areas. Once inside it, due to tensions, misunderstandings between Member States and also from outside it, due to events / actions outside the European Union, materialized in risks and threats generated by terrorism, the refugee crisis, political and military tensions, etc. Both areas from which these situations arose affected the security of the European Union and often influenced, unfavorably, the evolution of common projects and programs that were intended to improve relations between states and to increase citizens' quality of life.

Establishing common courses for action by the foreign policy of the EU Member States and ensuring a secure framework for the implementation of common projects and programs has involved several bodies within the Union's political system and several European institutions to ensure their legality. In order to act coherently, they have a unique vision and have established the most complex, comprehensive and effective strategies, meant to respond as timely as possible to the various risks and threats posed to the European security environment. As a result, European political cooperation brings into negotiations the foreign

[1] Augustin Fuerea, *Instituţiile Uniunii Europene,* Editura Universul Juridic, Bucureşti, 2002, p. 28.
[2] Federica Mogherini, *„A Global Strategy for the European Union's Foreign And Security Policy"*, conform http://eeas. europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, accessed on 24.08.2020.
[3] Jean-Claude Juncker, discursul despre Starea Uniunii 2016, *„Către o Europă mai bună – o Europă care protejează, capacitează și apără"*, 14.09.2016.

ministers of the EU Member States, that, under a mandate from the administrations of the countries of origin, have agreed to keep each other informed, within important meetings, about significant foreign policy issues and to adopt a common course of action and concrete measures to be decided unanimously by votes.

Following the adoption of this approach, it is decided that those issues related to foreign policy, and especially security, be included in an area in which collaboration and cooperation seek to ensure and defend national sovereignty, even if there are some differences between Member States that cannot be neglected, such as the possession of the nuclear arsenal or the membership / affiliation to other alliances and organizations.

The negotiations at the end of 1991 in Maastricht, where the Treaty on European Union took place[4], culminate in the adoption of new policies and forms of cooperation both between the Member States and between them and the structures, institutions, forums of the European Union and which do not lack aspects of EU's[5].foreign policy and security issues.

Thus, the European Council, through its new CFSP structure, sets out the objectives, broad lines and directions of action for common security, which are identified with the EU strategic interests, based on principles such as: protection of values, security and independence; democracy and human rights; peacekeeping and security; economic development; and poverty eradication. The European Parliament also plays an important role in the functioning of the CFSP, which monitors and contributes to the development of this structure, including through budgetary allocations necessary for the implementation of its programs and projects.

A conclusion that emerges from the presentation of this short history and the picture that frames the CFSP, can be supported by the statement that: CFSP focused on EU values, based on principles that form the foundation of the "EU Pantheon"; it is guided by clearly established objectives, and the courses of action it implements aim at their fulfillment; it constantly adapts to the geopolitical environment and acts visually, anticipating the changes, actions and situations that may affect the European security environment. This conclusion supports the need for the regular elaboration and full implementation of a Global Strategy for the European Union's Foreign and Security Policy[6], a strategy that is in a continuous and complex process of adaptation in all areas, of repositioning and redefining relations and positions in the matrix of the security environment and which must not deviate from the initial objectives of European security and the European citizens.

Nowadays, the EU has a strategy centered on a common vision that aims to complete a stronger and more secure Union than ever before. The current international challenges and the enlargement of the EU to the East of the European continent are shaping an increasingly unstable and insecure security environment, and these realities directly affect the lives of European citizens. The Global Strategy for the European Union's Foreign and Security Policy was developed in 2016 and its implementation involved representatives of academia, civil society, security specialists, all, together with representatives of the structures coordinating the CFSP, analyzed and discussed in meetings and conferences the general context, the immediate evolution, and the impact of current events on the European security environment.

---

[4] A.N.: Tratatul de la Maastricht denumit și Tratatul privind Uniunea Europeană a fost semnat în februarie 1992 și a intrat în vigoare în noiembrie 1993, conform https://europa.eu/european-union/law/treaties_ro, accessed on 24.08.2020.

[5] *Tratatele Uniunii Europene – versiune consolidată,* Editura Universul Juridic, București, 2013, pp. 29-30.

[6] *** *Viziune comună, acțiuni comune: o Europă mai puternică. O strategie globală pentru politica externă și de securitate a Uniunii Europene*, 2016, https://eeas.europa.eu/sites/eeas/files/language_versions_0.zip

Following the draft of this strategy, reports were prepared detailing the implementation of the strategy, the level reached, and the progress made in areas such as defense and security, state and societal resilience in the neighborhood, the integrated approach of crises and conflicts, and, most importantly, the directions have been designed and a common vision for the direction of the CFSP has been outlined in the coming years. It should also be noted that, soon after the elaboration of the strategy, a European action plan[7] aimed at the field of defense was presented at the level of EU decision-making forums, which highlighted the need to implement at national level, for all EU Member States, the acquisition, development and investment procedures, in land, air, sea and space defense capabilities.

2. Europe's Security Strategy and the design of an European army

Strategies have existed since ancient times. They still exist today and are found in all areas and at all levels of society. When there is a desire, a vital need to be achieved, or an ideal to be reached at any cost, a strategy is needed, to respond to clear and well-defined objectives. If we refer to "military strategy" we approach a vast field, that of military art, where we find aspects related to planning, training and fighting, all to achieve the goal, namely, the victory.

The military field has been, since its definition and establishment, an area where the phrase "military strategy" has been used. The term was a characteristic attributed to commandants, generals and was defined as „the means by which a commander can defend his own territory and defeat enemies"[8]. But later, in order to develop a military strategy, to devise war plans to achieve victory, it proved necessary to have a rigorous analysis of the battlefield, a detailed study of the enemy and an estimate of his possibilities, a logical order of activities, a vision and a capacity to anticipate the effects of future military actions, depending on the results of current or near future missions. It requires strategic thinking, careful calculations, and decisions based on logical reasoning. Thus the term "strategy" acquires the valences of a science, of an art with the help of which surprising results can be obtained, even in a totally unfavorable general context.

Another extremely important area where well-defined strategies need to be designed and implemented is the field of security. Starting from the simple to complex, from human needs, as they are ordered in Maslow's Pyramid, and analyzing the second level, "the need for personal safety and security"[9], we can design a simple form of a security strategy. If we amplify this need at the group level, society, or state level, we move from the individual need, which is designated to ensure the physical security and mental comfort, to a form of strategy, "multidimensional, flexible"[10] one, meant to ensure „a broad perspective on all systems"[11].

The present gives us an extremely complex and diverse picture of the world in which we live. Recent problems around the world require different strategies depending on the size of the risks and threats that spread to humanity. Europe cannot distance itself from global problems and events and it is working towards a firm and adaptable strategy, designed to respond to situations for which there is a vision in their evolution and for which Europe has defined its position. It must demonstrate also that it is ready at any time to act „if international

[7] *** *Implementation Plan on Security and Defence*, Council of the European Union, Brussels, 14 November 2016, https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf
[8] Lawrence Freedman, *Strategia, o istorie completă,* Editura Litera, București, 2018, pp. 113-114.
[9] Abraham Maslow, *Motivație și personalitate*, Editura Trei, București, 2013, pp. 167-179.
[10] Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*, București, 2020, p.11.
[11] *Ibidem.*

developments so require in order to define the strategic lines of the Union's policy in relation to that development"[12] so established since 1991, by the Maastricht Treaty.

Thus, the present Global Strategy for European Union's Foreign and Security Policy addresses extremely important areas in the field of security and defense, in which special emphasis is placed on state and societal resilience, in the field of existing crises and conflicts, where an integrated approach to or in the field of regional order and cooperation, where rules referring to multilateralism are in force, both internally and externally.

Security and defense is one of the areas for which Europe has allocated substantial funds by investing in new programs and projects (500 million EURO for the European Defense Industrial Development Program for the period 2019-2020 and another 90 million EURO for preparing actions in the field of defense research[13]), that aims to build a common, strong, and modern defense industry that ensures the security, autonomy and defense of the European Union. At the same time, the NATO-EU partnership has not been neglected, in which joint programs and exercises are developed, where strategies are aimed at military mobility, command and communication at a strategic level and projections are drawn up, cyber security visions, hybrid warfare and asymmetric threats are outlined. All these show that Europe is concerned and invests in the field of defense, especially in the defense industry, being the second after the US in terms of investment. But, there are some gaps which should be eliminated in the future in order to say that there is a secure strong Europe from a military perspective. Issues still to be addressed are related to the low level of technical and procedural interoperability between the armies of EU Member States, the existence of significant technological and operating systems gaps in the C4I sector and especially the existence of differences regarding the level of allocations of financial funds to the defense budgets of European countries.

A strong European army, guarantor of regional security and peace, was a desideratum launched in the years immediately following the end of the Second World War, when by the Treaty of Brussels of 1948, later amended by the Paris Agreement of 1954, the participant countries would decide that they provide mutual assistance if a Member State was the victim of an aggression. This decision determines the establishment of the Western European Union (WEU)[14], a military alliance that, since 1998, can allocate missions to the European Task Force (EUROFOR), an operational force composed of several multinational force structures.

The expansion of the EU and the majority membership of the EU Member States in NATO led to the dissolution of the WEU in 2011 and the strengthening of commitments and cooperation with the strongest military Alliance, which undertook to protect the security and defend the Member States. The development of common collective defense capabilities remains for Europe, a direction on which the Common Security and Defense Policy and its constituent structures focus, and of these, the European External Action Service has the role of pursuing the common foreign and security policy and to promote the EU's values and interests in international politics by increasing visibility and strengthening the coherence of actions.

The visions of the EU's defense strategies envisage a European army, complementary, not against NATO, as European political leaders claim, a solution to current risks and threats,

[12] Tratatul de la Maastricht, conform https://europa.eu/european-union/law/treaties_ro, accessed on 24.08.2020.
[13] Conform URL: https://ec.europa.eu/romania/news/20200406_fondul_european_de_aparare_ro, accessed on 24.08.2020.
[14] A.N.: Uniunea Europei Occidentale sau Uniunea Vest-Europeană s-a constituit ca şi organizaţie internaţională şi alianţă militară între şapte state membre NATO şi aliate cu SUA: Anglia, Franţa, Belgia, Luxemburg, Olanda, Italia şi Germania de Vest – conform Simon Usherwood, John Pinder, *Uniunea Europeană – O foarte scurtă introducere*, Editura Litera, Bucureşti, 2020.

a solution that can hardly be realized due to technological, economic and political differences between Member States. The core of this future army already coagulates in the European Union Forces (EUFOR), a military structure involved in more than 15 international missions, which regularly conducts joint training and exercises in which personnel of the Member States participate together with an already established subunit, the Multinational Battalion.[15].

One conclusion is that in order to neutralize current and future risks and threats, EU must continue the process of organizing and maintaining a military force ready at any time to be deployed in areas where the situation requires. But, the road to a European army is extremely difficult. It is hoped that it would be set up, but it is not possible yet, and until this goal is achieved, clarity, determination, and vision in European decisions, cohesion, cooperation, and understanding between all Member States and an immediate, strong, and decisive reaction from all Member States is needed to counter the risks and threats to the safety and security of Europe.

3. The Corona virus pandemic, another disease of the European security system

The beginning of 2020 see Europe in full process of intensifying security and defense action, new channels of cooperation be opened and negotiations be held to resolve the situations caused by Brexit, the implementation of the Global Foreign Policy and Security Strategy continue and funds be allocated for identifying small and medium enterprises that can offer new and revolutionary solutions in the field of defense. Services, trade in goods, construction and business began a new year, clauses in older contracts were honored, and other contracts were negotiated and started. Money and people move freely through a secure European community that guarantees and ensures their security.

The news that in the city of Wuhan[16] the festivities of the Chinese New Year, which is celebrated on January 25th, will take place quietly, in a partially closed city, with the population isolated in houses due to a sudden disease, a virus that easily spreads among people, also reaches the European continent, in a Europe that is too preoccupied with internal affairs and will later be accused of reacting late and hard to the future pandemic.

The emergence of the virus in East Asia and especially in China, a country with a communist regime that prefers to hide the truth internally and misinform externally any action, activity, or phenomenon that is not to the liking of the Communist Party, has also done more difficult to prepare a strategy to limit the spread and control of COVID-19. The spread of the virus proves that it is not doing politics and all attempts by China to hide its existence and spread are drowning in the absurd and derisory. The World Health Organization, warned by officials of the Taiwanese Public Health Service, is aware of the virus, but is extremely credible with the report of the Wuhan Health Commission, which presents insufficient data and states that there is no evidence that it is would transmit from man to man.

The true reality is understood immediately, when the virus can no longer be controlled and an exponential spread takes place, and its spread globally gives it all the characteristics of a pandemic.

[15] A.N.: Batalionul multinaţional - subunitate ce are în compunere aproximativ 2000 de militari, cu rolul de forţă de reacţie rapidă, gata oricând să intervină la declanşarea unei crize neaşteptate, conform https://www.europarl.europa.eu/ news/ro/headlines/security/20190612STO54310/apararea-va-crea-ue-o-armata-europeana, accessed on 24.08.2020.

[16] A.N.: Oraşul Wuhan – Capitala provinciei Hubei din China Centrală, cu o populaţie de peste 11 milioane de locuitori, un important centru economic, politic, financiar, comercial, cultural şi educaţional, al nouălea oraş ca mărime din China, conform https://en.wikipedia.org/wiki/Wuhan, accessed on 24.09.2020.

Europe is hit by the relentless Corona virus pandemic. Medical systems in member countries are collapsing, hospitals are no longer able to cope with the wave of critically ill patients, governments are taking harsh measures, emergencies are being imposed, rules are being put in place and shops, schools and public institutions are closed. Europe's engines are stalled and the cohesion of the European Union is being put to the test. The national interest of the EU Member States in protecting their own population determines the closing of borders, the freezing of trade, even of the one with materials necessary for the sanitary system and the reorientation of the industry towards the production of medical devices, equipment and means of protection. The effects of the pandemic put pressure on the budgets of less developed countries and have a devastating impact on their economies, which are already in a deep coma.

The intervention of international institutions and organizations is expected, but they are taken unprepared and redirect the responsibility for the fight against the Corona virus pandemic to the governments of each nation. The European citizen is exposed to a danger he does not know how to avoid. His Europe is no longer secure, as promised, and his world and ours are a sick world living in isolation and physical distancing. The Corona virus pandemic has demolished the fortress of security and safety of the European citizen. The last bastion to put hope in, is the own country, and in this case the approaches are different from state to state. The European citizen no longer exists, and now there are differences and what sets us apart is self-evident. The economic level, the educational and cultural level, the involvement of the ruling political class that must convince its electorate that it has chosen well and last but not least the defense capabilities of each state and the involvement of the army in ensuring security and safety. Europe should wake up, harmonize these differences in order to receive another chance from the European citizen, hidden behind the mask of the pandemic that masks the feelings of fear and confusion.

At European level, the scourge of the coronavirus pandemic is infesting plans and affecting the EU's way of acting in the field of security. Important ongoing projects and initiatives launched to ensure a proper security climate are forced to reduce their budgets and reanalyze their business schedules. One of these kind of project's, the "Project on the enhanced integration of defense", which is part of the Permanent structured cooperation program, intended to set up the groups of armed forces necessary to strengthen European defense capacity has plans to deploy these forces to areas imminent crisis, which is why it needs a specific civilian and military infrastructure to ensure mobility. Thus, the EU encourages Member State governments to invest in this area and initially allocates a fund of 7.5 billion EUR. The amount is subsequently reduced by 60% due to the pressure exerted on the budgets of european countries by the expenditures incurred in combating the coronavirus pandemic, a measure that delays the project and even jeopardizes its completion[17].

The military budgets of the EU and NATO member states are being put to the test, so cooperation between these institutions suffers. The military exercise "Defender-Europe 20" planned to take place in 7 European countries will be carried out on a small scale. The US military also reduces the number of participants in the largest exercise at European level in the last 25 years, and at national level, the Ministry of Defense cancels the

[17] Ştefan Oprea, *O altă piesă a dominoului securităţii a căzut în faţa COVID-19*, conform https://monitorulapararii.ro/ o-alta-piesa-a-dominoului-securitatii-a-cazut-in-fata-covid-19-1-31841, accessed on 24.09.2020.

participation of the Romanian military in the Saber Strike and Swift Response exercises to be held in Estonia, Latvia and Georgia[18].

The economies and financial resources of EU countries are beginning a struggle for survival. The needs of medical systems require funds that were not provided for in budgets, and the inability of these systems to meet the challenges posed by the coronavirus pandemic outlines an older vulnerability of them and the ruling political classes who ignored the importance and needs of this sector.

The EU is putting in place mechanisms prepared for crisis response and demonstrating its commitment to involvement in this pandemic by setting up european financial support packages amounting to € 1.8 trillion[19].

Thus, the econo*m*ic recovery will be faster for the member countries, it will not leave traces at the social level as other economic crises have done and the most important thing is that it will demonstrate the existence of a strong, united and stable EU, an important geopolitical force regional and global security.

Conclusions

What exactly is this pandemic?

It is a full-fledged war. It is a confrontation with an unseen and extremely dangerous enemy, on a battlefield where our families, homes, and jobs are exposed. We are all on the defensive position, preparing for an attack in which we must engage responsibly and fight in order to win the reassuring feeling of security and safety.

What do we need?

Our weapons should be the self-consciousness and awareness that we have in front of us an enemy that carries out large-scale offensive actions, but we can annihilate it if we lift the mask from the principles and values long forgotten somewhere at the society low level. We should remember solidarity, good manners, respect, discipline and honor, values over which the political and economic interests, the need for power and the egos of each of us lay, and over which we should definitively establish a strong and impenetrable mask.

The consequences of the war with the COVID-19 pandemic will not disappear too quickly, the vulnerabilities produced in the economic, social and political systems will offer the possibility to assert and promote those who put their personal interests above security needs. It is possible to witness changes in parliamentary majorities, government overthrows, social movements and the discontent of the masses generated by the reality that after the pandemic the rich are even richer and the poor have become even poorer.

The European Union must have a much stronger structure, and the new strategies should be drawn up, with focus on directions of solidarity and cooperation in internal markets, on the efficient management of budgetary resources, on the promotion of common interests and respect for national values, alongside with ensuring security and foreign policy by resuming meetings between national decision-making forums. Post-pandemic Europe must be reborn "without a mask", stronger and more stable, more sincere and more pragmatic. Existing strategies need to be adapted to current changes and improved with the lessons learned from this pandemic war.

[18] Conform https://www.digi24.ro/stiri/armata-romana-isi-anuleaza-participarea-la-defender-europe-20-cel-mai-mare-exercitiu-militar-al-nato-programat-in-acest-an-1277481, accessed on 24.09.2020.

[19] Conform https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/overview-commissions-response ro, accessed on 24.09.2020.

BIBLIOGRAPHY:

1. ***, "Apărarea: va crea UE o armată europeană?", *Parlamentul European*, URL: https://www.europarl.europa.eu/news/ro/headlines/security/20190612STO54310/apararea-va-crea-ue-o-armata-europeana;
2. ***, JO C326, *Tratatele Uniunii Europene – versiune consolidată,* Editura Universul Juridic, Bucureşti, 2013;
3. *EU Global Strategy*, URL: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
4. FREEDMAN, Lawrence, *Strategia, o istorie completă,* Editura Litera, Bucureşti, 2018.
5. FUEREA, Augustin, *Instituţiile Uniunii Europene,* Editura Universul Juridic, Bucureşti, 2002.
6. MASLOW, Abraham, *Motivație și personalitate*, Editura Trei, București, 2013.
7. MOISESCU, Gabriel-Florin, *Coronacriza – Provocări pentru viitor!*, Revista Academiei de Ştiinţe ale Securităţii Naţionale, nr.1/2020, Editura Academiei de Ştiinţe ale Securităţii Naţionale, Bucureşti, 2020.
8. TODERAN, Olivia; CELAC, Sergiu; SCUTARU, George, *Lumea de mâine. Ce urmează după pandemie?*, Editura Curtea Veche, Bucureşti, 2020.
9. USHERWOOD, Simon; PINDER, John, *Uniunea Europeană – O foarte scurtă introducere,* Editura Litera, Bucureşti, 2020.

POSSIBLE WAY OF COMMUNICATION AND CONFLICT MANAGEMENT IN HEALTH CARE INSTITUTIONS

Gabriella RÁCZKEVY-DEÁK
Registered nurse, Biologist, International Security and Defence Policy Expert,
Ph.D. Candidate at Óbudai University Budapest, Hungary.
E-mail: raczkevy.deak.gabriella@phd.uni-obuda.hu

Abstract**:** *Nowadays, the frustration and fear caused by the COVID-19 leads to aggressive manifestations in all areas. Perhaps even more common in health care institutions. However, often not only the fear of this virus, but inadequate communication from health care workers leads to aggressive actions. Patients respond in a variety of ways to a sudden change in health or functioning. While some of them are open and grateful for care, others may express strong emotions. Some emotions expressed by patients are more difficult for health care personal to deal with. Common difficult interactions include patient expressions of emotions such as anger, anxiety, and depression, as responses to crises. These emotions could cause violent actions in health care institutions. The paper presents communication methods and strategies used in health care and looks for answers such as why verbal and non-verbal communication mistakes can cause physical, verbal aggression or conflict. It examines which communication method is more useful in dealing with conflict situations occurring in patient-doctor, nurse-patient interactions in health care. The article recommends types of communication. It highlights the importance of empathy since without it the conflict cannot be solved or it can only temporarily. The article also emphasizes that it would therefore be important to train staff in appropriate communication trainings as well as to practice these lessons in situational exercises.*

Keywords: *patient; conflict; aggression; health care; communication; hospital security.*

Introduction

Nowadays, the frustration and fear caused by the COVID-19 leads to aggressive manifestations in all areas. Perhaps even more common in health care institutions. However, often not only the fear of this virus, but inadequate communication from health care workers leads to aggressive actions. In my paper I present the communication methods used in doctor-patient and nurse-patient relationships in healthcare. I mention empathic, assertive, suggestive communication, and in more detail, the non-violent communication technique developed by Marshall Rosenberg. My goal is to explore how to prevent or deal with situations of aggression in health care, moreover, how to deal with emerging and existing conflicts. Aggression is a state of frustration, anger that develops in countless cases because health care workers are overworked, work in a stressful environment, and because of this, their inadequate communication causes dissatisfaction for other persons. When a person feels that his or her interests, values, needs, and sense of justice are being harmed in some form, it leads to a state of conflict.

Conflicts between nursing patients and relatives are most common in health care institutions, so in my article I mainly try to present the conflict situations between the patient-nurse in more detail and outline the possible answers to them. It should be taken into account

that 70-80% of employees in health care facilities are female and thus may be more likely to be victims of verbal and non-verbal violence, even sexual harassment. It is also characteristic that women are more likely to cause verbal violence, while men are more likely to cause physical violence. Verbal violence is much more common in health care than physical violence is, yet both can be prevented through effective communication. Aggression can disrupt the operation of hospitals and endanger the safety of workers, patients, or even relatives.[1]

In my paper I have used communication, nursing etc. expert's books, articles, internet content and my health care professional experiences as well.

1. Communication and conflict

Communication is the exchange of information in a human signal system. In communication, two parties act as transmitters and receivers, through multiple verbal and non-verbal channels in parallel. However, it is advisable to distinguish between the concepts of communication and interaction. Interaction has a deeper, broader meaning because when we interact with someone, we exchange meanings. On the other hand, it often happens that certain expressed ideas have different meanings for some people, as they are formed by personal experiences, cultural-value differences and therefore carry different emotions and interpretations. That is why it is important to understand each other well when exchanging reports. It is worth thinking about what the other person really meant, what they wanted to express. Did the receiver of the message understand and interpreted the message correctly? If this fails, a conflict situation emerges. We can only empathize with another person's state of mind and understand, but we will only be able to empathize if we are aware of certain meanings. Empathy is especially necessary in communication, as it is not a negligible consideration to correctly interpret the feelings conveyed by the communication of the other party. Words can be contradicted by nonverbal communication such as: tone, melody, emphasis, posture, facial expressions and gestures. Thus, the meaning of words can be dwarfed in identifying the other person's feelings.[2] But what are the feelings that can provoke conflicts? Lack of acceptance, certain stressful situations such as: frustration, helplessness, anger, insecurity, pain, mental wounds, feelings of vulnerability and struggle can create confrontations and in such cases there is a possibility of collision of some power systems. Both want different things and can develop competition between them. Internal or spiritual conflicts can also lead to external conflicts, in which case the person may be offended, humiliated or hurt, provoking aggression, confrontation and debate. It projects its internal instability onto the other.

When the parties aim for cooperation and it is the mutual interest of both parties, they should strive for mutual solutions. However, cooperative endeavours require trust, and that they treat one another with sufficient attention and patience, and that they support each other through open communication. Competitive and conflict-avoiding behaviours cannot resolve conflicts. Avoidance strategies on one party only postpone the resolution of the conflict and projects anxiety or frustration on the other party, who is weaker than him. In such cases, a

[1] Gabriella Deák: *Erőszak a kórházban*. In.: Military Security Office. Professional Rewiew. 2012.1.p. 190.
[2] Emőke Bagdy, Beáta Bishop, Csaba Böjte, Éva Rambala: *Empátia, kommunikáció, konfliktuskezelés*. Kulcslyuk Publisher. Budapest. 2011. pp.117-120.

subject with such a personality may attack and grumble. The competing personality type exacerbates confrontation, causing frustration for one or both parties to the conflict.[3]

Conflicts of power (due to down-regulation), negotiation, and socio-emotional conflicts (to protect identity, self-esteem, and beliefs) can occur in hospitals. Negative conflicts can be resolved through effective communication methods.

2. Concept of empathy

Empathy comes from the Greek word "*pathos,*" which means strong emotion, passion. The word first appeared in 19th century English texts and, according to Alfred Adler, means "*to see with the other person's eyes, to hear with the other person's ears, and to feel according to the other person's heart".*[4] Over time, empathy has been used only in the field of aesthetics and philosophy of art, and only as a concept of artistic experience interpretation. Carl. R Rogers was the first person who described a modern conception of empathy. Rogers was a well-known American psychologist who did a lot of research, writing, and doing to aid the helping professionals to understand and appreciate empathy. According to him, each person has a unique, behavioural and world of experience system with a specific internal frame of reference, a unique logic, which may even be quite different, which is assumed from the outside. Rogers wanted to understand this internal system. The manifestation of empathy also depends on the nature of the relationship between people and the will of the person experiencing empathy. Empathy is a weave of very many multifactorial processes.[5]

According to Rogers, empathy means, "*one enters the other's perceived world* […] *temporarily lives the other's life, walks tactfully in it, free from judgment."* So, empathy comes with understanding.[6]

We can see from the previous quotations that the condition for empathy is a direct communication relationship. This communication can be verbal or metacommunication. Thus, empathy can only be evoked by one communicating person from the other, which causes turnaround as well as attention. What is needed in the person turning around is an attitude that anticipates the assumption of positive qualities in the other person because he or she considers him or her valuable. This skill is a more complex form of interpersonal behaviour that can be learned, but its existence can be personality dependent. Empathy unfolds mainly in the process of interactions. A very important accessory is the line of communication between the practitioner, which can elicit different responses from the other party, since in itself one can measure every response to some internal expectation.

Empathy can be conscious or unconscious.

1. In the conscious, the "ego" comes under intentional control. It is the result of self-observation and self-education. Thus, empathy can be developed through teaching and practice.

2. By instinctive empathy, a person perceives and responds to the other's unique individual state. Such a person is sensitive to non-verbal communication, has a skill of attention to the person, and behaves honestly, authentically (congruently). If the behaviour is

[3] According to Thomas Kilman, five types of conflict management methods and personal traits are possible: competitive, problem-solving, avoiding, adaptive, and compromising. In.: Mészáros Aranka (editor): *Kommunikáció és konfliktusok kezelése a munkahelyen.* ELTE Eötvös Publisher. Budapest. 2007. pp. 256-257

[4] Béla Buda, *Empátia*. Urbis Publisher, Budapest, 2006, p. 11.

[5] *Ibidem,* pp. 11-35.

[6] Susan Smith, *Kommunikáció az ápolásban,* Medicina Publisher, Budapest, 2009, pp. 97-98.

credible, the other person will be more open, give more communication signals, and there will be room for empathy.[7]

How to communicate empathetically? Methods of empathic communication

The process of consent means the acceptance of the other party without judgment. Thus, from the other person, it causes relief, and the feeling of liberation that accompanies communication, so that one does not feel necessary to have to fight for the truth. Active listening and understanding are important, which is also related to empathy. The person providing the information feels through non-verbal communication (e.g. posture, eye contact, etc.) that the person receiving the information is listening in an understanding manner. Many have a natural intuition, but clinical empathy learned and applied in practice is a consciously used tool for the success of interventions. However, this requires the intention of the empathetic provider and the inclusion of the recipient.

For help, empathy transforms into a kind of verbal connection. However, this spiritual shift requires flexibility in the boundaries of the "I". The health care professional experiences and feels the patient's state of mind and plans what to say or do for the patient. The healthcare worker informs the patient that he understands his feelings and the cause of his temper. We should not diminish the significance of what is being said, so accuracy and punctuality are important in verbal experience. Not repeating the patient's words, but his own words and style should be used by the caregiver and showing this way that he or she has understood the patient's feelings. Proper vocabulary is important to avoid repetition of what the patient has said. Therefore, it is reasonable to master the synonyms of words expressing different emotions and apply them in everyday practice. In addition to the verbality of empathy, non-verbal communication is also very important. Speech containing comprehensible words will not be authentic if it is not accompanied by metacommunication: e.g. attentive posture and the accompanying emphasis. You can create the answer according to the requirement of accuracy and precision, without touching the other. It is important that speech is accompanied by understanding and honesty, excluding regret. Empathy is free from bias and judgment.

The book Communication in Nursing lists situations in which it is useful to apply empathic communication. The nurse should behave empathetically if the patient is confused, anxious, nervous, terrified, hurtful, insecure. During such communication, the rights of the patient's personality must be respected, and in order to avoid intrusion, it is necessary to consider propriety.[8]

My personal experience (ten years in healthcare) and several emergence cases have shown that empathic communication has positive effects: it reduces feelings of loneliness and isolation, it can create hope, dissolve alienation as empathy "*builds bridges toward our fellow human beings*". By communicating empathetically, the caregiver saves time, increases patient awareness, and feels accepted. Confidence in the nurse also increases if the patient feels that there is no prejudice on the part of the nurse. Moral prejudice is conflict-provoking as the other party begins to defend against it, attacks, or withdraws. The nurse's empathy can evoke positive feelings and change patients' behaviour. This prevents the patient from defending himself or justifying their feelings. If the nurse demonstrates enough understanding toward the patient, more aggressive behaviour and conflict can be more easily avoided and managed. Such an empathic question is, for example*: I see you are afraid of the examination. What can I do to dispel your fear?* The nurse's behaviour thus becomes like a psychotherapist, because if the patient hears the nurse's response to his or her feelings, he or she may become more aware of his or her inner world. The patient becomes aware of how to deal with the situation

[7] Buda, *Empátia*, pp. 183-184.
[8] Susan Smith, pp. 97-98.

and experiences more cooperation. The nurse is also positively affected by empathic behaviour, seeing the patient's cooperation as feedback is filled with satisfaction and compassion.

Requirements for empathic communication are as follows:

- it is important to avoid personal and private problems and thoughts,
- it is vital to pay attention to the speaker and, if possible, it is not advisable to appear impatient and interrupt the patient's verbal communication,
- it is important to focus on non-verbal messages as well, so that this way the message will be fully received,
- we should try to deduce the most important element of what the patient has to say - e.g. whether the speaker expresses scare, uncertainty etc.
- the sympathetic response must embody accuracy and precision and be consistent with metacommunication,
- it is necessary to pay attention to the patient's reception of the empathic question or answer, it is worth supporting this with another question, e.g.: Do I see the situation well?[9]

If the healthcare professional is not empathetic, caring and attentive, the patient's behaviour may change in a negative direction, e.g. she or he may feel frustrated, turn around, or start fighting his feelings attempt to convey it. When he turns to himself, he refuses to be effective.

3. Assertive communication

The ability to communicate assertively means being able to express one's thoughts and feelings with confidence while respecting the rights of others. It is characterized by sufficient determination and self-awareness and it strives to achieve its goals in harmony with its environment. The assertive communicator has self-knowledge and self-confidence through his / her orientation (questions), confident in his / her actions and behaviour. In certain situations, he can react with empathy, without temper, he can express his thoughts clearly and decisively, and if necessary he can even say no. He's expression of opinion is constructive, listens to the thoughts of others, and asks.[10]

According to the previous characteristics, a nurse who demonstrates an assertive form of behaviour, considering professional and job regulations, makes conscious decisions in her social and work matters and strives to deal with certain situations that arise during nursing. One such nurse does not allow others to take advantage of her seeks solutions to conflicts, and is actively involved in interactions with people. Self-assertive communication protects the rights of the individual and others at the same time, seeking consensus based on the facts, keeping in mind the most optimal solution acceptable to both parties. The patient treats negative emotions confidently: like anxiety, fear, manipulation, intrusion, and aggression. The patient attaches equal importance, the rights of himself and others, and knows how to behave in accordance with his own respect for himself and others. In this way, the person communicating clearly expresses his or her thoughts and feelings, thus avoiding confusing, easily misunderstood and offensive messages. His non-verbal communication is in harmony with the verbal, characterized by a soft tone, a confident, warm open look, the presence of eye

[9] *Ibidem*, pp. 99-103.
[10] Sabatina Disney, Anumol Joseph, "Assessment of self esteem and assertivness among nursing students", *Journal of psychiatric nursing*, no. 8(1) September 2019, URL: https://www.researchgate.net/publication/335543248_Assessment_of_self_esteem_and_assertivness_among_nursing_students, accessed on 02.05.2020.

contact, a relaxed posture, and a timely sloping of the limbs. Such a person values himself without underestimating others and is characterized by mutual respect.

If a person is unable to behave assertively, he or she can easily fail because he or she is unable to show respect for himself or herself and others. A person who communicates with a reluctant, timid behaviour presents the opportunity to be victimized. In contrast, aggressive communication is the loud expression of reaching a person for what they want, even to the detriment of others. In doing so, the aggressively communicating individual aggressively places his or her own expected rights above others. The aggressive party can be dismissive, hostile, abusive, even manipulative, and disrespects the feelings of others and disregards the right of others to be treated politely, respectfully, and fairly. This behaviour forces the other person to end the harm done to the person. The most common response to this could be an attack, a side-line or conflict avoidance. We can resolve the existing conflict only with self-assertion, assertive communication.

According to the book Communication in Nursing, the nurse should examine the source of aggression and the causal relationship with which it can open the way for dialogue. You can ask such questions e.g.: *I see that you are angry with me because…. Please tell me what annoyed you so much?*[11]

It is important for the attacker to be aware of the hurtful, aggressive nature of his behaviour and possibly its legal consequences. The healthcare worker will tell him openly, for example: *If you yell at me like this, it makes me uncomfortable and difficult to work with you*. It is important to have self-assertive communication here as well, to avoid humiliation. It is important to maintain calmness and self-control so that the patient can become aware of his or her own misbehaviour. The nurse should not tolerate attacks if he or she wants to maintain self-esteem and patient confidence. The author considers it important for the nurse to make a thorough assessment of the situation. The assertive nurse should explore the patient's thoughts, feelings, and expectations and communicate with him or her accordingly: What does the patient fear from? Does he feel threatened? Does he feel distrust, fear? Do she/he want or need to be safe, understand, and reassure the nurse?

The caregiver needs to rethink what communication strategy he or she uses in each situation. If you have done this effectively, then comes monitoring and evaluating the impact. In such cases, he should remain calm and empathetic, show respect, and reassure the patient that he or she is receiving professional and appropriate care. The healthcare professional should tell what and why he or she is doing to help the patient recover. It is best to ignore the patient's hurtful words and focus only on his or her needs.

4. Convincing communication

In persuasion, the primary goal of the information provider is to create lasting changes in the attitudes or opinions of the recipients. For the recipient, this communication strategy only achieves its purpose if he understands the communication and accepts its content and identifies with what is being said. The nature of three elements and their relationship to each other determine the success of communication. These are:

1. how authentic and reliable the source of the communication is;
2. what is the content and natural emotional acceptability of the communication;
3. what is the recipient of the communication (age, gender, information).[12]

[11] Lisa Kennedy Sheldon, *Communication for Nurses (Talking with patients)*, Second Edition, Jones and Bartlett Publishers, Sudbury, Massachusetts, 2009, p. 6.
[12] János Pilling (ed.), *Orvosi Kommunikáció*. Medicina Publisher. Budapest. 2008. p. 120.

This type of communication may occur more frequently in doctor-patient relationships and less frequently in nurse-patient relationships. The effect of communication can be submission or obedience, it can be identification with it (the recipient considers the information to be true) and it can become internal as the information is deeply embedded in the individual's principles. When structuring what is being said, the practitioner should follow the introduction and then elaborate on the speech and complete it. As feedback, to reinforce the understanding, the speaker can ask questions. Such communication is used by the doctor when he wants to persuade the patient to take the medication regularly or to agree to a surgery. Here, too, empathy must not be forgotten, because without it, it would only be a matter of will and decision. This communication can also be important in the development of compliance, cooperation in doctor-patient, nurse-patient relations. However, if not applied properly, the opposite effect can be achieved, communication can trigger defense from the patient and will show resistance or attack. A person using such method of communication should not use words such as: *Believe me, I know it should be taken this way*, or in a commanding tone: *Take it this way because it is because if not…* - these are condescending and even aggressive words. *If you don't take this, it will be very bad* - a statement is a negative suggestion, and it is not a persuasive strategy that produces a positive result. The patient can submit and carry out the instruction, but he does not feel that he has the freedom of choice, the right to decide on the treatment. Careful, accurate, and empathetic communication is also very important in this kind of interaction, too.

5. Suggestive communication

Suggestions are communication messages that trigger an involuntary response. These messages or responses can be negative or positive. In a suggestive message, if "*a message reaches and affects the recipient, the effect is essentially suggestive, since it does not fulfil the message or request voluntarily, but involuntarily."*[13] Negative suggestions should be avoided in healthcare. In most cases, the suggestion is given by the sender (sender of the message) and affects the recipient. But many times, unconsciously, negative or positive emotions can be triggered by a sentence, behaviour, and metacommunication because patients do not respond equally to suggestion and are often in a state of reduced or altered consciousness during an illness and more sensitive to certain modes of communication.

The provider often suffers from a lack of information, becoming insecure and terrified, hungry for signal, so the suggestive effects are more pronounced for him. When processing information for a patient, the interpretation or intent with which the practitioner sent the message does not matter, but rather how he or she encodes it as a recipient. It is characteristic of patients that in this altered state of mind, the message may be decoded differently, resulting in a negative suggestion. Thus, incorrectly chosen words have a negative effect on the patient. For instance, '*It will hurt you a lot.'* are honest words but as a nocebo effect can cause a lot of pain.[14] The opposite is the positive suggestion, which can have a very beneficial effect on patients and the effects of which have been proven by many studies. According to them,

[13] Katalin Varga, Csaba Diószeghy, *A szuggesztiók jelentősége az orvos – beteg kommunikációban.* In: János Pilling (ed) *Orvosi Kommunikáció*, Medicina Publisher, Budapest, 2008, pp. 149-153.

[14] Nocebo effect as well: if a patient believes that a drug will harm him, in many cases his condition will actually worsen, even if the drug he is taking is actually a placebo. In such cases, the drug without the active ingredient is called nocebo because it does not promise that I will "like it" (which is the original meaning of the word placebo), but that it will "harm me." Many times, the doctor inadvertently creates a nocebo effect, such as when he tells a patient, "It will never heal." In this case, the patient's condition may worsen from nocebo effect alone, or at least not as much as it could from treatment.http://pszichologia.phd.elte.hu/vedesek/koteles_ ferenc_phd.pdf, accessed on 13.12.2019.

positive suggestions can reduce pain and even speed up healing. They are also important in resolving conflicts, because if you empathetically suggest only positive feelings to the needs and feelings of the host party, and could reveal the cause of the conflict, you can resolve it.[15]

Thus, the efficiency of communication can be increased by suggestion elements. An important element is positivity, to highlight what is good from each intervention and to focus on what is pleasant, for example: *It will make you feel better or heal after this intervention, ...the test can treat your illness*, etc. The words need to be wrapped up in words that evoke dear positive feelings that mean '*I'm here, I'll help if you're in trouble, you can count on me'*. The style of this method of communication is usually permissive, but can even be dominant, depending on the personality of the host and what the situation requires. It is best to allow, as this makes the more empathetic e.g. *'If you do that… ..then you will find that…'*

Positive suggestion can be interwoven into all existing communication and made an integral part of every interaction. Words should always be chosen wisely and messages to the patient should be worded in such a way that they carry a positive message. I consider it important for healthcare professionals to learn some techniques of positive suggestive communication and thus help the patient heal faster and tolerate certain interventions more easily. With this knowledge, many misunderstandings and conflicts could be prevented.

6. Concept and use of non-violent communication

The concept of nonviolent communication was introduced by the American clinical psychologist Dr. Marshall B. Rosenberg, who wanted to develop an educational system that would make the opportunity for the world to acquire peace-building skills. Non-violent communication (hereinafter NVC) has proven to be an effective tool in the peaceful handling of certain differences of opinion. This method is a kind of empathic communication, but because it is well applicable to the prevention or treatment of violence, it has been given the name of non-violent or cooperative communication.

NVC is based on language and communication skills that help to maintain humane behaviour even in the most difficult situations. It shows how to change our way of expressing and how to listen to others effectively. Thus, words will be tools to express what we hear, feel, and want. It teaches us how to express ourselves honestly and respectfully while paying attention to the other with respect and compassion. With this method of communication, we recognize our own and the other person's needs. It teaches us not to attack, defend, or retreat as a result of criticism, but to express clearly what we feel, what we think, and what we need. This avoids being diagnosed or prejudiced. Its most important principle is to be with the other person. It has four components: The first is observation – communicating something to a person that does not involve prejudice or criticism. e.g. '*You argue with me …*'. The next step is to express our feelings about the problem '*which hurts me'*, and then '*we tell you what the need is for'* that expressed feeling: and '*it violates my need for happiness'*. The fourth step is to make a request: '*please don't do this'*. The four steps of NVC are observation, feelings, needs, and request. Part of the NVC is a very clear indication of information in words or other means. The other part is receiving information from the other person. Empathy is also very important in this method. This communication technique can be used in a wide variety of situations and is already used by some doctors (especially in Western countries) as it helps them to understand the needs of patients. NVC is also a tool for resolving violent conflicts. This method "*enhances the focus of attention, respect for the other, empathy, and the desire*

[15] Katalin Varga, Csaba Diószeghy, *A szuggesztiók jelentősége az orvos – beteg kommunikációban*. In: János Pilling (ed.), *Orvosi Kommunikáció*, Medicina Publisher, Budapest, 2008, pp. 153-157 and Katalin Varga (ed.), *A szavakon túl. Kommunikáció és szuggesztió az orvosi gyakorlatban*, Medicina Publisher, Budapest, 2011, pp. 29-33.

for the parties communicating with each other to give each other from the bottom of their hearts."[16]

By learning non-violent communication, communication errors can be undressed learned and entrenched, such as: making judgments, comparisons, denial of responsibility, or other blaming, claims that involve overt or covert reprimand or punishment. Many use a way of speaking in which they qualify, compare, demand, but talk little about their feelings and needs. NVC helps to recognize and avoid this way of speaking. The first component of the NVC is the separation of observation and expression, but if this is confused, the host party expects to hear criticism from what is being said. The second component of NVC is the expression of feelings. It can help resolve conflicts if we can name our feelings accurately and clearly e.g. *Does it make you angry that I care little about you?* or *It makes me angry that the nurse cares little about me*. In the third stage, the needs behind the feelings need to be made aware, because if someone criticizes a person, the critic can receive the reviewer's message by blaming himself or herself or blaming others. We should be aware that you are paying attention to the feelings and needs behind your own or the other person's criticism. Many people respond to criticism with self-defence or counterattack, but the better someone can relate their feelings to their needs, the easier it will be to respond to criticism with compassion. E.g. ..: '*I feel that you need safety and attention and that is why you talked to me like this'* or '*I feel that you are afraid and need safety and that is why I will do my best to provide this for you'*, or '*I have a lot of work now, but I'll be back in an hour and can we talk about this again"*?. If the nurse does not understand the patient, he or she can ask back. e.g. *'You mean, like, I'm not dealing with you?'* or '*I want to know what you think about this, do you want to tell me something else?'* The fourth element of NVC is how to communicate to the other. It is about what we should say and do in order to mutually enrich each other's lives. Empathy is also very important in this communication, and it does not mean giving advice, but devoting our full attention to the other person's message. Therefore, a nurse should give him the time and space so that he can fully express himself and so that he can feel that we fully understand him. The intellectual approach to a situation is not empathy. Similarly, empathy is not sympathy, as feeling is not about sympathy. Empathy is when we respond by using synonyms of the patient's feelings, almost completely repeating what the other said. It is very important to maintain empathy throughout communication, so you need to give the other enough time to talk. We cannot intervene, we cannot be impatient, as this prevents the speaker from expression. However, in order to give empathy to someone else, we also need to have and receive it.

Non-violent communication can be used to communicate with people with tense nerves and can also resolve situations that threaten violence. A very important rule is not to use the word *'but'* when speaking, for example*: 'But there is… but yes I know better... because'*. It is not effective and can even be dangerous to a violent person. However, applying NVC in a tense situation can prevent physical aggression. For example: '*You seem very angry and want to go home*.' Patient's possible answer: '*Yes, because no one here takes me notice of me'*. The healthcare worker's question: '*Are you tired of not paying attention to you, do you feel not respected, appreciated?'* The patient's answer*: 'Yes, and I feel .. Yes because…. etc'*. Most probably, if the violent patient can express what bothers or hurts him, we may be able to use empathic words to find a solution and offer it. Negative responses like '*not'* or *'do not want'* from the patient can be treated with this method of communication. The questioning emphasis is important in verbal communication because if we take it down, we seem to declare the conversation over.

[16] Marshall Rosenberger, *Nonviolent Communication: A Language of Life: Life-Changing Tools for Healthy Relationships (Nonviolent Communication Guides)* Third Edition, Puddle Dancer Press, 2015, pp. 10-22.

The following is an example of a violent situation caused by a demanding patient that a healthcare professional is trying to resolve with NVC:

Patient: *Leave me alone! You just run all day and every time I just ring, it doesn't come right away! What if I died in the meantime? You're not even a nurse!*

The nurse explains or attacks against NVC without using NVC, or uses the word but: *But you ring every five minutes and imagine I have twenty more patients besides you! or: What do you think of yourself, aren't you my only patient!?* This is an aggressive response.

Response from a nurse using NVC (because she knows the patient is afraid or lonely): '*Do you feel alone, lonely, and need attention'?* The patient's answer: '*Yes, you just keep running and don't care that I ring*.' Nurse: '*It shook what I heard from you and I want to understand you. Do you long for human dignity and respect*?' Patient: '*Yes*.' Nurse*: 'I want to help you. What can I do for you?'* The patient should not be rejected or responded to in a sharp, commanding tone of voice, neither should he be left behind, after all, the nurse also has feelings and needs. Here it is related to assertive communication, because the nurse also has a self, she is also there, but she wants to "connect" with the patient and feel her feelings and situation. She can only achieve this by communicating firmly so that she is not treated as a martyr by the patient but notice that the nurse is also there in the dialogue. Communication can mean the end of conflict, resolution and reconciliation.

From the previous example, we can see that this communication can also be an effective tool in preventing and treating acts of aggression in a hospital, however, it requires a lot of learning, patience, and practice. It can be learned by anyone through trainings where the learner learns this method of communication through various situational exercises. In my opinion, knowing this mode of communication is effective and even useful, although it is time consuming to learn, practice, and use for a nurse who is busy working with many patients. Physicians also have little time to talk to the patient, but once NVC is properly practiced, a conflict can be treated very quickly so that it does not escalate and grow from verbal to physical violence. As I see it, the only downside is its time-consuming nature. Therefore, if we want to apply NVC well, we must provide the patient sufficient time for the expression of their feelings and needs.

7. The role of nonverbal communication in causing conflict

In this section, I will most often cover meta-communication situations that are incorrectly used among physicians, as I have personally experienced these phenomena during my many years as healthcare worker and as a patient.

Meta-communication is extremely important to avoid aggression and frustration, as our main intention is to avoid confrontation and aggression with our gestures and behaviours. The body must convey the same message as verbal communication as this makes our message authentic. But if the behaviour of the practitioner is not authentic enough, it can increase the intensity of the conflict. In the following, I propose a solution to use correct nonverbal communication.

First, taking up proper posture plays a significant role in communicating with the patient. Efforts should be made to always reach a height level with the patient, considering the patient's body position (sitting or lying down), as it is very important to keep eye contact at the same level. If we look down on the patient, he may feel inferior, if we look up, he may feel like a leader. Sit next to the patient's bed in the ward, or if we are in the office, not facing the patient, but at a 60-degree angle, forming an open triangle with the patient (this is the cooperative situation). It is reasonable to position yourself so that the patient's facial features are visible during the conversation, and the face does not express rigor, the facial features

should be kind, slightly smiling, suggestive of empathy. Cross-arms should be avoided as this can lead to alienation from the patient's needs and suggest a sense of superiority.[17] The sound should be soft, not too quiet or loud, the speech should be articulated, medium speed. During the communication, the message of tilting the head sends to the outside world about openness and friendship – in practice it is worth using this. Cross-twisting of the lower limbs is not recommended either, because it perceives protection and withdrawal from the patient's problems. The patient should be watched and looked into the eyes, but not wolf's eyes, because it can encourage an attack or cause anxiety or frustration in some people. The subject should not go on an adventure because it can mean boredom and inattention. Looking over the glasses can indicate espionage and judgment. This negative feeling can be avoided by removing the glasses or using them as intended.

A polite handshake and introduction are important when the patient arrives. In my work in healthcare, I have found that in many cases this does not happen. Behind the desk, many doctors greet the patient in a strictly commanding tone without introduction. His/her questions and answers do not radiate empathy, they are characterized by rigor and a commanding, intolerant tone. Positioning in front of the talking partner creates a defensive, rival atmosphere. The desk is a railing and the patient is in tension, she/he can feel the other side of the desk. It would be justified to place it close to the patient in a triangle with the chair. In many cases, the anamnesis is also recorded in a prompt tone and the information about the treatment is convincing. In this case, the patient may feel that he or she has no decision-making power and may lose control of his or her own body and recovery, and a dominant behaviour may allow for attack as well as a high degree of anxiety from the patient. The behaviour of nurses can have a similar effect if they communicate with the patient in a commanding tone, in a non-selective style. If the patient feels that his or her person is neglected and not adequately involved in his or her own recovery, he or she cannot cooperate.

It is often the case that the attending physician looks down on the sitting or lying patient during the daily visit to the ward, prompts him not to ask for certain movements, but it is not uncommon for him to communicate impatiently, using scientific language - which the patient is unable to follow or understand. This mode of communication can trigger aggression or introversion from the patient. During hospital treatment, physicians should better involve the patient in treatment. It would be more empathetic to sit next to the patient, ask him in a kind tone, and be careful not to violate his intimacy and privacy rights. Communicating with your hands behind you in a standing position is also contraindicated, as this is the so-called princely pose and send the message 'not to approach'. Hands on the hips are among the most spectacular signs of territorial dominance, but in addition to making sense of ownership, they also signal that there are serious problems with someone's attitude. A characteristic element of medical non-verbal behaviour is the so-called "bedside manners", which usually show a bit of forced gentleness, friendliness, with frequent touches such as patting on the shoulder or face. These manners can evoke a treated feeling from the patient, as it is a movement like when a father pats his little son's shoulder, so the doctor treats the other person as an unequal party.

It is often absent from medical empathy, care, and patience – not all of which can be traced back to poor income conditions and overwork, but can often be the result of fatigue, burnout – and these are shaping the conflict. By mastering and practicing appropriate empathic, non-violent, suggestive communication techniques, they can be avoided and the conflicts that arise can be largely managed. Increased mental and financial support for

[17] John, Navarro, *The Dictionary of Body Language: A Field Guide to Human Behavior*, Harper Collins Publisher, 2018, United States of America, pp. 9-27.

employees and the introduction of motivational methods could also be indirectly conflict-preventing.

Conclusion

In my article, I tried to present communication strategies that are consciously or instinctively used in health care and the communication situations practiced by an existing patient health care professional, which are sometimes incorrect in many cases. I suggested and introduced in practice what I consider the more effective method of communication (non-violent communication method). Applying this method of communication, we would be able to eliminate the emerging conflicts and resolve the existing ones in the short and long term. There are several overlaps between the communication methods presented, and most have empathy as a principle. Failure to empathize only causes harm in patient care and this does not help to resolve conflicts, but further enhances their deepening.

In the healthcare professional-patient relationship, persuasive communication can, in my opinion, violate patient decision-making rights, if not openly, manipulation is created by communication. I am ambivalent about this method of communication. In my present writing, for reasons of length, I do not attempt to explore the subjective factors that, in many cases, due to the strong lobby of drug manufacturers, the physician prescribes a patient for treatment that is not warranted to treat the patient. The doctor persuades the patient to make a good decision. But I recognize that in justified cases, persuasion is necessary for the effectiveness of certain treatments, as this will have a positive effect on the patient, as without non-compliance would occur, which could endanger the patient's life or recovery.

The communication advantage of a self-advocate is that the health care professional does not communicate as a victim, but with enough self-confidence and professionalism, communicates much more effectively with the patient or relative, and strives for a consensual solution as an equal party.

Suggestive communication, if we use only the positive side, can only have benefits during care. The patient becomes calmer by it and feels less urge to attack.

Empathic as well as non-violent communication follow the same communication strategy, their central guideline is empathy. In both communication strategies, the receiving party accepts feelings and both parties strive for prejudice-free communication. Prejudice, blaming, defamatory styles should be avoided when managing conflicts, as this can be a source of conflict. Understanding attention and empathy is always needed. In resolving conflicts, it is important for the partner to feel that our actions include the promise of a compromise negotiation leading to a solution. It is important to respect the other, to express emotions, and to acknowledge mistakes. The strategy outlined above cannot have this disadvantage in that it is time-consuming to resolve the conflict. In Hungarian healthcare, the doctors and the nurses have little time to talk to the patient, so it is not certain that this method will resolve the conflict in this short time. And impatience is another form of verbal violence that can trigger an aggressive counterattack. Unfortunately, there are few health facilities today that have adequate time and material and human resources to treat and provide information to patients.

I consider it important to handle the conflicts with appropriate communication techniques, as constructive conflict resolution increases the self-confidence, authority and human esteem of the health professional. To avoid aggression, we can combine some communication strategies depending on the situation, but once formed, I consider empathic or non-violent communication to be the most appropriate communication method. Self-assertion is needed for all types of communication, without it only one or both parties can fall victim to

a conflict, and this is a destructive method of conflict management. Destructive conflict management results in anxiety, conflict avoidance, or deepening of existing conflicts, which can manifest in the form of psychosomatic illnesses in the long run. This is detrimental to the individual, the institution and the quality of patient care.

It would therefore be very important to train staff in appropriate communication trainings as well as to practice these lessons in situational exercises. My article describes these types of communication, from which I would highlight empathic and non-violent communication as a very useful method to master.

BIBLIOGRAPHY:

1. ANGELO, Elizabeth, *Managing interpersonal conflict*, Nursing Management, 2019, URL: file:///C:/Users/rgy/Downloads/Managing_interpersonal_conflict__Steps_for_success.7.pdf
2. *Assertive Techniques for Conflict Resolution*, URL: https://exploringyourmind.com/assertive-techniques-for-conflict-resolution/
3. BAGDY, Emőke; BISHOP, Beáta; BÖJTE, Csaba; RAMBALA, Éva, *Empátia, kommunikáció, konfliktuskezelés*, Kulcslyuk Publisher, Budapest, 2011.
4. BERCKHAN Barbara, *Verbális Önvédelem*. Bioenergetic Publisher, Budapest, 2011.
5. BIRKENBIHL, Vera F., *Kommunikációs gyakorlatok*, Trivium Publisher, Budapest, 1998.
6. BUDA, Béla, *A közvetlen emberi kommunikáció szabályszerűségei:* URL: http://www.mek.oszk.hu/02000/02009/02009.htm#32
7. BUDA, Béla, *Empátia.* Urbis Kiadó, Budapest, 2006.
8. DEÁK, Gabriella, "Erőszak a kórházban*"*, in *Military Security Office, Professional Review*, 2012/1, Budapest.
9. DISNEY, Sabatina, ANUMOL Joseph, *Assessment of self esteem and assertivness among nursing students*, Journal of psychiatric nursing 8(1), September 2019, URL: https://www.researchgate.net/publication/335543248_Assessment_of_self_esteem_and_assertivness_among_nursing_students
10. HALLER, József, *Miért agresszív az ember?*, Osiris Publisher. Budapest, 2005.
11. MÉSZÁROS, Aranka (ed.), *Kommunikáció és konfliktusok kezelése a munkahelyen*, ELTE Eötvös Publisher, Budapest, 2007.
12. NAVARRO, Joe, *The Dictionary of Body Language: A Field Guide to Human Behavior*, Harper Collins Publisher, United States of America, 2018.
13. PILLING, János (ed.) *Orvosi Kommunikáció*, Medicina Publisher, Budapest, 2008.
14. ROSENBERGER, Marshall, *Nonviolent Communication: A Language of Life: Life-Changing Tools for Healthy Relationships (Nonviolent Communication Guides)*, Third Edition, Puddle Dancer Press, 2015.
15. SALIMBENE, Suzanne, *What Language Does Your Patiente Hurt in?*, Paradigm Publishing, USA, 2005.
16. SHELDON, Lisa Kennedy, *Communication for Nurses (Talking with patients)*, Second Edition, Jones and Bartlett Publishers, Sudbury, Massachusetts, 2009.
17. SMITH, Susan, *Kommunikáció az ápolásban*, Medicina Publisher, Budapest, 2009.
18. TAMPAROAND, Carol. D.; WILBURTA, Q. Lindh, *Therapeutic Communications for Health Care*, Delmar Learning, USA, 2008.
19. TRINGER, László, *Gyógyító beszélgetés*, Medicina Publisher, Budapest, 2007.
20. TÚRI, Viktória, "A konfliktuskezelés nemi különbségeinek a vizsgálata", in *Bolyai Rewiew*, 2009/3/1, URL: http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/3/01_turiviktoria.pdf
21. VARGA, Katalin (ed.), *A szavakon túl. Kommunikáció és szuggesztió az orvosi gyakorlatban*, Medicina Publisher, Budapest, 2011.

VIEWS ON THE MANAGEMENT OF THE CURRENT PANDEMIC CRISIS

Tiberiu TĂNASE, Ph.D.
Assistant Professor, Romanian-American University, Bucharest, Romania.
E-mail: tiberiu_tanase@yahoo.com

Ovidiu BOUREANU
Master's student, Management-Marketing Faculty, Romanian-American University, Bucharest. Romania. E-mail: oboureanu2003@yahoo.com.

Abstract*: In this paper we have focused on the major challenge of the 21st century, namely the COVID-19 viral pandemic. We aimed to analyze the vast problem from several angles using resources from media, international and local organizations, global reflection centers, think tanks and others. Our aim was to search on the subject and evidence the role played by the international organizations in the fight against the pandemic COVID-19. We also evaluate the situation and challenges in the field of public health that influences national security, affecting the citizens state of health, nations and national states. After a period of 100 years of free pandemic, our world is in uncharted teritories as the new virus COVID 19 become an omnipresent element of grave concern.*

Keywords*: COVID-19; SARS virus; ONU; national security; international security.*

Introduction

First cases of confirmed COVID-19 infections have occurred in European Member States starting January 2020. Few weeks later on 30 January 2020 the United States is reporting its first confirmed case of COVID-19. On the same day, the WHO declare that the outbreak is a public health emergency and a matter of international concern. By the end of February 2020, Italy announced a significant increase in COVID-19 cases, then on 11th of March 2020, the WHO declares that the new outbreak of COVID-19 is a pandemic[1].

There are currently two major hypotheses about the appearance of the virus: it was transmitted from bat to human, through another intermediate animal, or a second hypotheses less probable – it and accidentally escaped from an laboratory[2].

1. Early warnings of/from the intelligence services

The German Federal Office for Civil Protection has been issued warnings since 2012[3] about a potential health crisis caused by a virus that could lead to the collapse of the healthcare system, but the warning was not echoed, as no one was interested. Under the

[1] *Timeline: WHO's COVID-19 response*, URL:https://www.who.int/emergencies/diseases/novel-coronavirus-2019/interactive-timeline, accessed on October 02, 2020.
[2] *Coronavirus disease 2019 (COVID-19), Situation Report – 94*, URL: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200423-sitrep-94-covid-19.pdf, accessed on October 02, 2020.
[3] *Germany Overview of the National Disaster Management System*, URL: https://ec.europa.eu/echo/what/civil-protection/disaster-management/germany_en, accessed on September 08, 2020.

coordination of the Robert Koch Institute, experts wrote scenarios on the assumption that Germany would be hit by an epidemic[4].

The pathogen was called "Modi-Sars" and was based on the Sars virus. ”The symptoms were fever and dry cough, most patients have difficulty breathing, the radiographs show changes of the lungs"[5] is shown in the report. The consequences in such a scenario would be the shortage of medical equipment, but also of personnel, and the sanitary services reaching collapse. The report was received by the parliamentarians and the ministers, but without effect. As in the case of annual risk evaluations, this report was not seriously discussed either. The head of the Federal Office for Civil Protection Christoph Unger declared for the newspaper Frankfurter Allgemeine Zeitung: ”Extremely important steps in the risk management process were missing"[6].

The U.S. intelligence agencies issued classified warnings of the global danger posed by coronavirus since January and February. The intelligence reports did not predict when the virus would reach the United States and did not made recommendations on measures that public health officials should take, as they are not issues within the competence of intelligence agencies[7].

Reports and warnings created an early image of a virus showing the characteristics of a pandemic that encompasses the entire globe, which may require rapid action to be limited. Despite the steady stream of reports, Trump has continued to publicly and privately downplay the COVID-19 threat to Americans. Also, US lawmakers did not face the virus until March, when officials demanded that citizens stay in their homes[8]. But in the USA there is also National Center for Medical Intelligence, a subdivision of Defense Intelligence Agency specialized in medical intelligence, which obtained information about the epidemic in Wuhan since November 2019[9]. Subsequently, the decision-makers were informed since February of this year that this outbreak poses a major pandemic risk, a warning issued before the World Health Organization (WHO). A similar warning was issued in January 2020 by the medical intelligence department of the Canadian Military Intelligence Service (CFINTCOM)[10].

Although not the first documented pandemic to affect the globe, COVID-19 is the first "digital" pandemic - the world has never been so connected, so it is expected that there will be unprecedented challenges, including for the intelligence/defence community. For the intelligence services, it can be a double challenge - threats can spread rapidly in this hyperdense network of connections characteristic of the current world in crisis (ex. epidemics, strategic disinformation operations, cyber attacks), but solutions can spread just as quickly[11].

---

[4] *Modeling the spread of COVID-19 in Germany: Early assessment and possible scenarios*, Published online 2020 Sep 4, URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7473552/, accessed on October 02, 2020.
[5] *Ibidem.*
[6] DD, “Experții germani avertizau, în 2012, asupra unei crize similare coronavirusului”, *HotNews*, URL: https://www.hotnews.ro/stiri-coronavirus-23791791-raport-expertii-germani-avertizau-2012-asupra-unei-crize-similare-coronavirusului.htm, last accessed on October 02, 2020.
[7] *Modeling the spread of COVID-19 in Germany... op. cit.*
[8] ***, “Serviciile de informatii americane au avertizat inca din ianuarie februarie despre riscul aparitiei unei pandemii”, URL: https://financialintelligence.ro/serviciile-de-informatii-americane-au-avertizat-inca-din-ianuarie-februarie-despre-riscul-aparitiei-unei-pandemii/
[9] Mara Stroescu, “COVID-19 şi serviciile secrete (II)”, April 21, 2020, *Analize*, Cosmin Dugan, URL: https://larics.ro/covid-19-si-serviciile-secrete-ii/, last accessed on October 03, 2020.
[10] Murray Brewster, “Canadian military intelligence unit issued warning about Wuhan outbreak back in January work is raising new questions about what the government knew and when”, *CBC*, Apr 10, 2020 URL: https://www.cbc.ca/news/politics/coronavirus-pandemic-covid-canadian-military-intelligence-wuhan-1.5528381, accessed on October 05, 2020.
[11] Mara Stroescu, *COVID-19 şi serviciile secrete (II)*, *op.cit.*

2. Is the pandemic a current threat to international security?

The threat was caused by the spread of COVID-19 virus by delaying protection measures, being non-compliant with isolation, etc. which until now were considered topics concerning the medical structures and infrastructures of the states more than the effort of the UN Agencies. On the other hand, specific advances and the proliferation of biological weapons of all kinds make the survival of some states threatened by events that often occur on the territory of another state, as is now the case of the virus/pandemic that left China and affects the whole world, particularly Europe and USA.

Addressing the 15-member body on the impact of COVID-19 on international peace and security, the Secretary-General of the United Nations, Mr Antonio Guterres said the health pandemic was rapidly becoming a protection crisis. "Our collective security and our common well-being are being attacked on many fronts"[12] he said, "driven by a relentless disease and sustained by global fragility. Our challenge is to save lives today, while supporting the pillars of security for tomorrow"[13].

The effectiveness in the fight against COVID-19 requires a more active effort and role on the part of traditional actors, and the WHO needs to strengthen international law and increase global cooperation and solidarity. Thus, the UN Secretary-General called on all countries to "intensify their efforts immediately" to fight the coronavirus pandemic. UN Secretary-General, Antonio Guterres, on March 12 called on all countries to "step up their efforts immediately to fight the coronavirus pandemic"[14].

"I call on every government (...) to step up its efforts - immediately"[15] he said in a statement. "Because this crisis is affecting everyone, we all have a role to play"[16] he added. Antonio Guterres sees the WHO statement as: "a call to action, for everyone, everywhere"[17] .The UN chief said in a statement: "It is also a call for responsibility and solidarity"(...)"While we are fighting the virus, we cannot let fear spread"[18]. The UN chief insisted: "Together we can still change the course of this pandemic"[19].

3. What is the WHO capable of and what is it doing?

Speaking at a press conference at the UN Office in Geneva, on March 25, 2020, the World Health Organization spokeswoman Margaret Harris warned that the number of victims of the COVID-19 epidemic in the world will increase significantly. Noting that as the current epidemic continues to spread rapidly, the official indicated that the worst epidemic to date

[12] COVID-19, "Profoundly Affecting Peace across the Globe', (Says Secretary-General, in Address to Security Council), 2 July 2020, URL: https://www.un.org/press/en/2020/sc14241.doc.htm, last accessed on October 05, 2020.
[13] *Ibidem.*
[14] ***, "Secretarul general al ONU a facut apel la toate tarile sa isi intensifice eforturile imediat pentru a lupta impotriva pandemiei de coronavirus", URL: http://stiri.tvr.ro/secretarul-general-al-onu-a-facut-apel-la-toate-tarile-sa-isi-intensifice-eforturile-imediat-pentru-a-lupta-impotriva-pandemiei-de-coronavirus_857504.html# view, 12 March 2020, last accessed on October 06, 2020.
[15] *Ibidem.*
[16] Maria Stan, "ONU mesaj de mobilizare anti-coronavirus: Împreună putem încă schimba cursul acestei pandemii", 12/03/2020, URL: https://www.stiripesurse.ro/onu-mesaj-de-mobilizare-anti-coronavirus-impreuna-putem-inca-schimba-cursul-acestei-pandemii_1439586.html, last accessed on October 07, 2020.
[17] *Ibidem*.
[18] *Ibidem.*
[19] *Ibidem.*

was triggered by the Ebola virus in West Africa and has resulted in 11,000 deaths in two years[20], is proving that the world is indeed facing a huge epidemic.

Pointing out that Europe and the US have become the areas most affected by the pandemic, Harris pointed out that ”85% of the total number of cases reported in the last 24 hours come from Europe and US”[21].

The spokeswoman said that measures such as traffic restrictions and quarantine taken by some countries could slow the spread of the epidemic, insisting that medical institutions and their employees would gain time as a result of said measures. Asked if the US would become a new epicentre of the COVID-19 pandemic, Harris said the number of cases of infection with COVID-19 had increased significantly, noting that this potential existed[22]. The state of emergency posed by the Global Pandemic brings into question a special problem of Western society: how to respond: with a defensive or offensive strategy? The fight against the pandemic, in any form, requires a new way of understanding security, without defining geographical boundaries, the effectiveness of this fight involves undertaking preventive activities, in which case the role of the United Nations must be fundamental.

Mr. António Guterres, Secretary-General of the United Nations, said that COVID-19 revealed the fragility of the world. It has plundered the most vulnerable and erased decades of progress. For the first time in 30 years, poverty is on the rise, nuclear non-proliferation efforts are declining, and countries are failing to act in areas of emerging danger, especially in cyberspace. "Our world is struggling, it is stressed and it is looking for real leadership"[23] he said, stressing: "We are in a fundamental moment"[24].

The United Nations efforts to combat pandemics must be guided by the strategies adopted by the Member States as soon as possible. Thus, as a United Nations strategy to combat the pandemic, the Global Plan for Humanitarian Response in the Context of COVID-19 was adopted, which will be coordinated by the United Nations Office for the Coordination of Humanitarian Affairs[25].

This plan meets the requirements of several organizations: the World Health Organization (WHO), the Food and Agriculture Organization (FAO), the International Organization for Migration (IOM), the United Nations Development Program (UNDP), the United Nations Population Fund (UNFPA), The UN Human Settlements Program (UN-Habitat), the UN Refugee Agency (UNHCR), the United Nations Children's Fund (UNICEF) and the World Food Program (WFP)[26]. Mention should be made of the warning of the UN Humanitarian Coordinator, who said that if vulnerable countries are not helped to fight the

[20] ***, “85% of New Infections, Deaths Coming from Europe and US”, *UN*, March 24, 2020, URL: https://www.voanews.com/science-health/coronavirus-outbreak/un-85-new-infections-deaths-coming-europe-and-us, last accessed on Octomber 15, 2020.
[21] Emma Farge, Stephanie Nebehay, “United States could become coronavirus epicenter”, *WHO*, March 24, 2020, URL: https://www.reuters.com/article/us-health-coronavirus-who-usa-idUSKBN21B1FT.
[22] ***, “Secretarul general al ONU”, *op. cit.*
[23] ***, *Describing COVID-19 Pandemic as Wake-Up Call, Dress Rehearsal for Future Challenges, Secretary-General Opens Annual General Assembly Debate with Vision for Solidarity*, 22 September 2020, URL: https://www.un.org/press/en/2020/ga12268.doc.htm, last accessed on October 04, 2020.
[24] *Ibidem.*
[25] ***, “Alte agenţii ONU”, *UNHCR*, URL: https://www.unhcr.org/ro/homepage/guverne-si-parteneri/alte-agentii-onu, last accessed on October 08, 2020.
[26] ***, “Global Humanitarian Response Plan COVID-19”, *United Nations Coordinated Appeal*, April – December 2020, URL: https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Humanitarian%20Response%20Plan%20COVID-19.pdf, last accessed on October 11, 2020.

coronavirus now, millions of people could be at risk and the virus will circulate uncontrollably around the world[27].

In this context, the UN launches a $ 2 billion global humanitarian response to combat COVID-19 in 51 countries in South America, Africa, the Middle East and Asia, and urges governments to strongly support the global humanitarian response plan and allocate funds to ongoing humanitarian calls[28].

Thus, the Secretary-General of the United Nations, António Guterres, launched on March 25, 2020 a global plan on coordinated humanitarian response, worth $ 2 billion, to combat COVID-19 in some of the world's most vulnerable countries, already facing humanitarian crises due to conflict, natural disasters or climate change, in an effort to protect millions of people and stop the uncontrolled spread of the virus around the world.

The response plan will be implemented by UN agencies, together with international NGOs and non-governmental consortia that play a direct role in the response. It will allow: the delivery of essential laboratory equipment for testing and medical equipment for treating patients; installation of equipment for washing hands in camps and locations; launching information campaigns on how to protect yourself and others from the virus; creating bridges and overhead nodes in Africa, Asia and Latin America to transport humanitarian workers and supplies where they are most needed.

In this context, the Secretary-General of the United Nations, António Guterres, also stated: "COVID-19 threatens all of humanity, therefore all of humanity must retaliate. Individual country responses will not be enough. We need to help the most vulnerable, millions and millions who cannot protect themselves. Such an approach is related to human solidarity. This is the time when we need to take a step forward towards the vulnerable"[29].

The Under-Secretary-General for Humanitarian Affairs, Mark Lowcock considers COVID-19 has completely distraught the lives of the people in some of the richest countries in the world. Now, the virus reaches places where people are trapped in war zones, do not have easy access to clean water and soap, and cannot hope for a hospital bed if they fall ill and reach critical condition. It would be cruel and reckless to leave the poorest and most vulnerable countries to fate. If we allow the coronavirus to spread freely in these places, we will expose millions of people to increased risk, entire regions will sink into chaos, and the virus will be able to travel around the world again. States fighting the pandemic on their own territory give priority to people in their own communities, as expected. But the cruel truth is that they will not be able to protect their population if they do not act now to help the poorest countries protect themselves. Properly funded, our efforts to implement a global response will provide humanitarian organizations with the tools they need to fight the virus, save lives and help stop the spread of COVID-19 around the world[30].

---

[27] ***, "Planul global privind răspunsul umanitar în contextul COVID-19. Abordarea globală reprezintă singurul mod de a combate COVID-19, conform ONU care lansează un plan privind răspunsul umanitar", *UNICEF*, 25 March 2020, URL: https://www.unicef.org/romania/ro/comunicate-de-pres%C4%83/planul-global-privind-r%C4%83spunsulumanitar-%C 3 %AEn-contextul-covid-19, last accessed on October 05, 2020.

[28] ***, "ONU lansează Planul global umanitar în contextul COVID-19", 30 March 2020, URL: https://aquastiri.ro/2020/03/30/onu-lanseaza-planul-global-umanitar-in-contextul-covid-19/ last accessed on October 12, 2020.

[29] ***, "COVID-19, ONU lansează un plan global în valoare de două miliarde de euro privind răspunsul umanitar coordonat", 25 March, URL: https://www.bursa.ro/covid-19-onu-lanseaza-un-plan-global-in-valoare-de-doua-miliarde-de-euro-privind-raspunsul-umanitar-coordonat-02042930., last accessed on October 13, 2020.

[30] Mark Lowcock and Tedros Adhanom Ghebreyesus, "The coronavirus threatens all of humanity. All of humanity must fight back." March 25, 2020, URL: https://www.washingtonpost.com/opinions/global-opinions/wealthy-nations-pandemic-fight-doesnt-stop-at-their-borders/2020/03/24/94afdae8-6e0c-11ea-b148-e4ce3fbd85b5_story.html

Moreover, WHO Director-General Dr Tedros Adhanom Ghebreyesus said: "The virus is now spreading to countries with poor health systems, including some that are already facing humanitarian crises. These states need our support, not only for reasons of solidarity but also to protect us all and to suppress this pandemic. At the same time, we must not fight the pandemic by ignoring other health and humanitarian emergencies"[31].

In her speech, UNICEF Executive Director Henrietta H. Fore said: "Children are the hidden victims of the COVID-19 pandemic. Compulsory isolation and school closure affect education, mental health and access to basic health care. The risk of exploitation and abuse is higher than ever, both for boys and girls. For immigrant children or those living in conflict zones, the consequences will be unprecedented. We must not abandon them"[32].

Together, they called on UN member states to help reduce the impact of COVID-19 in vulnerable countries and stop the spread of the virus worldwide, by providing the strongest possible support for the plan, while supporting existing humanitarian appeals that help more than 100 million people whose survival depends on the humanitarian assistance provided by the UN.

Member States have been warned that any misappropriation of funds for ongoing humanitarian operations would lead to the creation of an environment in which cholera, measles and meningitis could spread, where even more children could become malnourished and where extremists could take control - an environment that would be an extremely fertile ground for coronavirus[33].

Moreover, this new Central Emergency Response Fund (CERF) allocation – one of the most consistent ever achieved – will help the World Food Program (WFP) ensure the continuity of supply chains and the transportation of humanitarian workers and humanitarian aid, the WHO to stop the spread of the pandemic, and other agencies to provide humanitarian aid and protection to those most affected by the pandemic, including women and girls, refugees and internally displaced persons. Support will include food security, physical and mental health, water and sanitation, nutrition and protection[34].

4. What could be said about COVID-19-post-COVID predictions

Global strategists imply that, after the COVID-19 pandemic, we will come face to face with a changed world[35].

From their conclusions, we selected the following:

A joint report by the Food and Agriculture Organization of the United Nations (FAO) and the World Food Program (WFP) warns that around 135 million people worldwide, from 55 countries affected by conflict and climate problems, have been on the verge of starvation in 2019, the danger is now aggravated by the pandemic, says the UN[36].

Ikenberry, professor at Princeton University, warns us about the diverse ideological landscape, similar to that of the 1930s and 1940s. He claims: that after any economic crisis, at the exit from the COVID-19 pandemic we will wake up in the midst of even more fragmented

[31] ***, "ONU lansează Planul global umanitar...", *op.cit.*

[32] ***, "Nu lăsați copiii să devină victime ascunse ale pandemiei de COVID-19", *UNICEF*, 13 April 2020, URL: https://www.unicef.org/romania/ro/comunicate-de-pres%C4%83/unicef-nu-l%C4%83sa%C8%9Bi-copiii-s%C4%83-devin%C4%83-victime-ascunse-ale-pandemiei-de-covid-19 , last accessed on October 12, 2020.

[33] *Ibidem.*

[34] ***, "Planul global privind răspunsul umanitar în contextul COVID-19...", *op.cit.*

[35]***, "Predictions of analysts everywhere", quoted by political newspapers Foreign Policy and Politico, URL: https://www.politico.eu/tag/foreign-policy/, last accessed on October 10, 2020.

[36] *Revista presei internaţionale,* 24 aprilie 2020, Postat de A. C., 24/04/2020, URL: http://www.rador.ro/2020/04/24/revista-presei-internationale-24-aprilie-2020/, last accessed on October 02, 2020.

societies than today. After an extremely nationalist, perhaps even xenophobic, boiling point of the "us with us for us" type, Ikenberry anticipates that the states of the world will recover. The functioning of multinational political bodies (such as NATO, the UN or the EU) will be rethought. In the long run, democratic countries will win[37].

Economically, COVID-19 complicated things even more: the production factories closed, as a result of which the medical, pharmaceutical, food chains, etc. are in a dive. In the next period, it is likely that small and medium-sized companies will sell some of their shares. It is believed that we will have many state interventions in the economy, a different kind of dialogue between the state and the private. It is quite possible that the inevitable global recession will be followed by an economic depression at the same macro level. About eating habits, Paul Freedman, a history professor at Yale, adds something about this change: "In Europe and America, sumptuous restaurants will lose ground to bistros. The era of home cooking is starting again."[38] Then, a virtual-real war is expected: between people who will claim a quasi-total return to physical life, as it was in the early 2000s, when digital media had not colonized free time, and groups that on the contrary, will campaign for the continuation of online professional life[39].

We will have to become more responsible with the common goods. Artificial intelligence, radiation, the growth of the planet's ocean, pollution, species extinction, computer viruses and viruses: we have learned on our own how global issues have global consequences. which we will have to face together, without throwing the dead cat in the yard of our overseas neighbours. But here a paradox is born. Joseph S. Nye Jr., a professor at Harvard asks: "Each country will take care of its national interest, which will amplify the global problems, which will remain nobody's. How do we get out of this?"[40].

New power relations between states, deepening pre-existing conflicts. John Allen, a former NATO commander said: "As always, history will be written by the victors of the COVID-19 crisis"[41]. Basically, those states that overcome the first humanitarian crisis, regardless of their pre-pandemic status, can set the tone for a new geopolitical game, at will.

On a financial market that is shrinking day by day, experts predict a slight shift to what is called planned economy in socialism. It is also expected to revive domestic industries, domestic production. It doesn't work like that now - an experiment that some countries might continue. Laurie Garrett, a former senior fellow for global health at the Council on Foreign Relations and a Pulitzer Prize winning science writer said: "COVID-19 showed us that pathogens not only make people sick, but economies as well"[42].

According to cultural critic Virginia Heffernan[43] , more and more employees will give up working overtime and other "success recipes" from motivational books[44] . The post-

---

[37] G. John Ikenberry, "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s", *International Organization*, Vol. 40, No. 1 (Winter, 1986), pp. 105-137, The MIT Press, URL: https://www.jstor.org/stable/2706744?seq=1, last accessed on October 01, 2020.

[38] Bess Connolly, *Yale historian Paul Freedman on the history of American restaurants and the 'paradox' of food*, May 5, 2017, URL: https://news.yale.edu/2017/05/05/yale-historian-paul-freedman-history-american-restaurants-and-paradox-food, last accessed on October 01, 2020.

[39] *Ibidem.*

[40] Joseph S. Nye, *How Do Past Presidents Rank in Foreign Policy?*, URL:https://harvardmagazine.com/podcast/2020/joseph-s-nye, last accessed on October 01, 2020.

[41] John Allen, *The History of COVID-19 Will Be Written by the Victors*, URL: https://foreignpolicy.com/2020/03/20/world-order-after-coronavirus-pandemic/, last accessed on October 01, 2020.

[42] *America's Health Future: The Impact of COVID-19 on our Health Systems*, Oct. 13, 2020, URL:https://www.washingtonpost.com/washington-post-live/2020/10/13/americas-health-future/, last accessed on October 01, 2020.

[43] Virginia Heffernan, *Twitter*, URL: https://twitter.com/page 88.

COVID-19 man will be more unleashed and free, will take more care of health, sleep and nutrition. In the balance of what makes us feel good about ourselves, passions and a kind of dolce far niente will weigh harder than career.

But very importantly, "Coronavirus will return to the scientist (doctor, researcher, inventor, professor, etc.) the long-lost podium."[45] The truth, through its most eminent emissary, science, will once again take a place of honour, committing its long exile on the fringes of a global society intoxicated by false news, conspiracy theories, anachronism, and the literature of facts. Analysts anticipate the decline of relativism, opinionism, subjectivity – I think that! – with valid argument claims. Let's expect a more real-world.

Conclusions

With the world facing an unprecedented threat, there is an opportunity to emerge with stronger health systems, and improved global collaboration to face the next health threat. As we focus on the immediate response to the COVID-19 crisis, it is important to keep in mind the breadth and depth of consequences already being felt across the globe. We must learn the lessons of this pandemic now and, in so doing, ensure that our response, wherever possible, leaves a lasting positive legacy, and makes the world of the future a safer place[46].

In conclusion, it is necessary to build an international order in which countries and people are integrated into a world where common interests and values prevail: human dignity, respect for the law, respect for individual freedom, market economy and free initiative, religious tolerance. It must be understood that a world in which these values are assimilated as standards and not as exceptions is the best antidote to the proliferation of terrorism.

The victory against the threat of the pandemic will not be a singular and punctual moment, but a lasting, sustained effort of the international community. Victory will be assured and long-lasting as long as the international community remains vigilant, will fight and cooperate uninterruptedly, in order to prevent the occurrence and spread of the effects of pandemics.

BIBLIOGRAPHY:

1. ALLEN John, *The History of COVID-19 Will Be Written by the Victors*, available at https://foreignpolicy.com/2020/03/20/world-order-after-coroanvirus-pandemic/
2. *Alte agenții ONU, Oficiul Națiunilor Unite pentru Coordonarea Afacerilor Umanitare*, availble at https://www.unhcr.org/ro/homepage/guverne-si-parteneri/alte-agentii-onu
3. *America's Health Future: The Impact of COVID-19 on our Health Systems*, Oct. 13, 2020, available at https://www.washingtonpost.com/washington-post-live/2020/10/13/americas-health-future/

[44] Virginia Heffernan, *Magic And Loss, The Internet As Art*, June 7, 2016, URL: https://www.kirkusreviews.com/book-reviews/virginia-heffernan/magic-and-loss/, last accessed on October 01, 2020.

[45] *How the World Will Look After the Coronavirus Pandemic: The pandemic will change the world forever. We asked 12 leading global thinkers for their predictions*, March 20, 2020, Foreign Policy-Analysis, URL: https://foreignpolicy.com/2020/03/20/world-order-after-coroanvirus-pandemic/, last accessed on October 08, 2020.

[46] *COVID-19 Strategy Update*, URL: https://www.who.int/docs/default-source/coronaviruse/covid-strategy-update-14april2020.pdf?sfvrsn=29da3ba0_19, last accessed on October 08, 2020.

4. BREWSTER Murray, *Canadian military intelligence unit issued warning about Wuhan outbreak back in January work is raising new questions about what the government knew and when*, CBC, Posted: Apr 10, 2020 4:00 AM ET. available at https://www.cbc.ca/news/politics/coronavirus-pandemic-covid-canadian-military-intelligence-wuhan-1.5528381
5. CONNOLLY Bess, *Yale historian Paul Freedman on the history of American restaurants and the 'paradox' of food*, may 5, 2017, available at https://news.yale.edu/2017/05/05/yale-historian-paul-freedman-history-american-restaurants-and-paradox-food
6. *Coronavirus disease 2019 (COVID-19), Situation Report – 94*, available at: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200423-sitrep-94-covid-19.pdf
7. *COVID-19 'Profoundly Affecting Peace across the Globe', Says Secretary-General, in Address to Security Council*, 2 July 2020, available at https://www.un.org/press/en/2020/sc14241.doc.htm
8. *COVID-19, ONU lansează un plan global în valoare de două miliarde de euro privind răspunsul umanitar coordonat*, 25 martie, available at https://www.bursa.ro/covid-19-onu-lanseaza-un-plan-global-in-valoare-de-doua-miliarde-de-euro-privind-raspunsul-umanitar-coordonat-02042930
9. *Describing COVID-19 Pandemic as Wake-Up Call, Dress Rehearsal for Future Challenges, Secretary-General Opens Annual General Assembly Debate with Vision for Solidarity*, 22 September 2020, available at https://www.un.org/press/en/2020/ga12268.doc.htm
10. FARGE Emma; NEBEHAY Stephanie, *United States could become coronavirus epicenter: WHO*, March 24, 2020, available at https://www.reuters.com/article/us-health-coronavirus-who-usa-idUSKBN21B1FT
11. G. John Ikenberry International Organization Vol. 40, No. 1 (Winter, 1986), pp. 105-137 (33 pages) Published By: The MIT Press - available at https://www.jstor.org/stable/2706744?seq=1
12. *Germany Overview of the National Disaster Management System*, available at https://ec.europa.eu/echo/what/civil-protection/disaster-management/germany_en
13. *Global Humanitarian Response Plan COVID-19*, United Nations Coordinated Appeal, april – december 2020, available at https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Humanitarian%20Response%20Plan%20COVID-19.pdf
14. HEFFERNAN Virginia, available at https://twitter.com/page88
15. HEFFERNAN Virginia, *Magic And Loss, The Internet As Art*, June 7, 2016, available at https://www.kirkusreviews.com/book-reviews/virginia-heffernan/magic-and-loss/
16. *How the World Will Look After the Coronavirus Pandemic: The pandemic will change the world forever. We asked 12 leading global thinkers for their predictions*, March 20, 2020, Foreign Policy-Analysis, available at https://foreignpolicy.com/2020/03/20/world-order-after-coroanvirus-pandemic/,https://www.unicef.org/romania/ro/comunicate-de-pres%C4%83/planul-global-privind-r%C4%83spunsul-umanitar-%C3%AEn-contextul-covid-19
17. LOWCOCK Mark; GHEBREYESUS Tedros Adhanom, "*The coronavirus threatens all of humanity. All of humanity must fight back.*" March 25, 2020, available at https://www.washingtonpost.com/opinions/global-opinions/wealthy-nations-pandemic-fight-doesnt-stop-at-their-borders/2020/03/24/94afdae8-6e0c-11ea-b148-e4ce3fbd85b5_story.html
18. *Modeling the spread of COVID-19 in Germany: Early assessment and possible scenarios*, Published online 2020 Sep 4. doi: 10.1371/journal.pone.0238559, available at https://www.ncbi. nlm.nih.gov/pmc/articles/PMC7473552/
19. NYE Joseph S, *How Do Past Presidents Rank in Foreign Policy?*, available at https://harvardmagazine.com/podcast/2020/joseph-s-nye
20. *ONU lansează Planul global privind răspunsul umanitar în contextul COVID-19*, 25 mart. 2020, available at https://www.europafm.ro/onu-lanseaza-planul-global-privind-raspunsul-umanitar-in-contextul-covid-19/
21. *ONU lansează Planul global umanitar în contextul COVID-19*, 30 martie 2020, available at https://aquastiri.ro/2020/03/30/onu-lanseaza-planul-global-umanitar-in-contextul-covid-19/

22. *Planul global privind răspunsul umanitar în contextul COVID-19. Abordarea globală reprezintă singurul mod de a combate COVID-19, conform ONU care lansează un plan privind răspunsul umanitar*, 25 Martie 2020, available at https://www.unicef.org/romania/ro/comunicate-de-pres%C4%83/planul-global-privind-r%C4%83spunsul-umanitar-%C3%AEn-contextul-covid-19
23. *Predictions of analysts everywhere*, quoted by political newspapers Foreign Policy and Politico, available at https://www.politico.eu/tag/foreign-policy/
24. Primele cazuri în Germania au fost raportate la sfârșitul lunii ianuarie 2020. Începând cu 17 aprilie 2020, Institutul Robert Koch (pe scurt: RKI) numără peste 130.000 de infecții confirmate și aproximativ 4.000 de decese în Germania, available at https://www.hotnews.ro/stiri-coronavirus-23791791-raport-expertii-germani-avertizau-2012-asupra-unei-crize-similare-coronavirusului.htm
25. *Revista presei internaționale*, 24 aprilie 2020, Postat de A. C., 24/04/2020, available at http://www.rador.ro/2020/04/24/revista-presei-internationale-24-aprilie-2020/
26. *Secretarul general al ONU a facut apel la toate tarile sa isi intensifice eforturile imediat pentru a lupta impotriva pandemiei de coronavirus*, available at http://stiri.tvr.ro/secretarul-general-al-onu-a-facut-apel-la-toate-tarile-sa-isi-intensifice-eforturile-imediat-pentru-a-lupta-impotriva-pandemiei-de-coronavirus_857504.html#view, 12 March 2020.
27. *Secretarul general al ONU a facut apel la toate tarile sa isi intensifice eforturile imediat pentru a lupta impotriva pandemiei de coronavirus*, available at http://stiri.tvr.ro/secretarul-general-al-onu-a-facut-apel-la-toate-tarile-sa-isi-intensifice-eforturile-imediat-pentru-a-lupta-impotriva-pandemiei-de-coronavirus_857504.html#view
28. *Serviciile de informatii americane au avertizat inca din ianuarie februarie despre riscul aparitiei unei pandemii*, available at https://financialintelligence.ro/serviciile-de-informatii-americane-au-avertizat-inca-din-ianuarie-februarie-despre-riscul-aparitiei-unei-pandemii/
29. STAN Maria, *ONU mesaj de mobilizare anti-coronavirus impreuna putem inca schimba cursul acestei pandemii*, 12/03/2020, available at https://www.stiripesurse.ro/onu-mesaj-de-mobilizare-anti-coronavirus-impreuna-putem-inca-schimba-cursul-acestei-pandemii_1439586.html
30. STROESCU Mara, *COVID-19 şi serviciile secrete (II)*, apr. 21, 2020, Analize, Cosmin Dugan, available at https://larics.ro/covid-19-si-serviciile-secrete-ii/
31. *The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s*, *Timeline: WHO's COVID-19 response*, available at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/interactive-timeline
32. *UN: 85% of New Infections, Deaths Coming From Europe and US*, March 24, 2020 09:56 AM, available at https://www.voanews.com/science-health/coronavirus-outbreak/un-85-new-infections-deaths-coming-europe-and-us
33. *UNICEF: Nu lăsați copiii să devină victime ascunse ale pandemiei de COVID-19*, 13 Aprilie 2020, available at https://www.unicef.org/romania/ro/comunicate-de-pres%C4%83/unicef-nu-l%C4%83sa%C8%9Bi-copiii-s%C4%83-devin%C4%83-victime-ascunse-ale-pandemiei-de-covid-19

POTENTIAL NEW SOURCES OF POWER IN INTERNATIONAL POLITICS. CASE STUDY: COVID-19 PANDEMIC AND HEALTH RESOURCES

Alexandra SARCINSCHI, Ph.D.
Senior Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania.
E-mail: sarcinschi.alexandra@unap.ro

Abstract: *This paper argues that there is a potential new source of power, especially of hard power, that is specific to contemporary security environment characterized by the threat of COVID-19 pandemic. The starting premise is that the health system resources are a potential new source of hard power for a state actor to promote its foreign policy based on inducements or rewards. In terms of J. S. Nye Jr., health system resources might be used as a bribe or promise not for military or economic assistance (as specific to hard power), but for medical/humanitarian assistance. Therefore, the paper starts with a brief theoretical overview of the power concept and sources of power and continues with an analysis of the way in which a pandemic affects the international politics, especially the COVID-19 one.*

Keywords: *state; power; hard power; health resources; competition for health resources and medical supplies; vaccine nationalism; vaccine diplomacy.*

1. Theoretical approach: state, power, and sources of power

The theoretical approach, in this paper, starts with Realism, but it does not exclude its critics and limitations.

Realists argue that *state* is still the most important actor in the international arena even if there are significant voices who say that other actors or social forces are impairing state sovereignty making it less relevant[1]. For instance, Liberalism postulates that although state is important, there are other actors that are able to influence the international agenda and to oversee the state (international organizations, non-governmental organizations, multinational corporations, terrorist groups, etc.). Also, other theories accept various levels of analysis that explain the world politics: Idealism deals with the individual, Liberalism – the state, Neorealism and Neoidealism – the international system, Poststructuralism – the language, Marxism – the class and finance capital, etc.[2]

These theories on international politics are using a central concept, namely *power*, that, despite its tradition, still is not proper conceptualized. For instance, Robert Keohane, a

[1] Stephen M. Walt, "The Realist Guide to the Coronavirus Outbreak", in *Foreign Policy*, 9 March 2020, URL: https://foreignpolicy.com/2020/03/09/coronavirus-economy-globalization-virus-icu-realism/, accessed on 05.10.2020.

[2] David A. Baldwin, "Power and International Relations", in *Handbook of International Relations*, Walter Carlsnaes, Thomas Risse, and Beth A. Simmons (Eds.), SAGE Publications, 2013, pp. 273-297, URL: https://scholar.princeton.edu/dbaldwin/selected-articles, accessed on 10.10.2020; Stephen McGlinchey, Rosie Walters, Christian Scheinplfug (Eds.), *International Relations Theory*, E-International Relations, Bristol, 2017; John A. Vasquez, *The Power of Power Politics. From Classical Realism to Neotraditionalism*, Cambridge University Press, 2004.

representative of the Neoliberalism, argues that the power of the state is disciplined by international institutions and arrangements created by states that have common and convergent interests[3]. At the other pole of the theoretical approaches is Constructivism stating that international politics must not be explained in terms of power, but in terms of "causal significance of learning and persuasion"[4]. As seen, there is no clear operationalization of the concept of power, but theoretical frameworks of what power should not be.

In this respect, Michael Barnett and Raymond Duvall[5] argue that Realism is the center of gravity in defining power and this definition - power as states ability to use material resources in order to make others to do what they otherwise won't do[6] - is central. Moreover, the taxonomies of power are starting from the realist one: "soft power" as opposed to "hard power", or "go-it-alone power" as a modification of realist approaches[7].

Developing their own analytical framework, Barnett and Duvall identify two dimensions of power that correspond to four types of power. One dimension is referring to "the polar positions of social relations of interaction and social relations of constitution" and the other one is specificity, meaning "the degree to which the social relations through which power works are direct and socially specific or indirect and socially diffuse"[8]. Consequently, the four types of power are: compulsory power (power as interaction relations or direct control of one actor on other), institutional power (power as indirect control of one actor on others by diffuse relations of interaction), structural power (power as capacity built in direct structural relations between actors), and productive power (the socially diffuse production of subjectivity in systems of meaning and signification)[9]. The authors argue that those four types of power are providing the answer to one of the most important questions in international politics: "in what respects are actors able to determine their fate, and how is that ability limited or enhanced through social relations with others?"[10].

Realists and neoliberals offer a framework for analyzing power by another taxonomy: hard power (Realism), soft power and smart power (Neoliberalism).

Hard power, as power to coerce, corresponds to realists' approach that underlines the importance of military and economic means in achieving foreign policy goals[11]. Thus, the economic capabilities are to be used for inducements, and the military capabilities - in coercion and command in order to achieve the foreign policy goals.

Soft power is a concept brought to the attention by Joseph S. Nye, Jr., one of the most important representative of Neorealism. Soft power is associated with intangible factors such

[3] Robert Keohane and Lisa Martin, "The Promise of Institutionalist Theory", in *International Organization*, No. 20 (1)/1995, pp. 39-51, DOI: 10.2307/2539214, accessed on 05.10.2020.
[4] Peter Katzenstein (Ed.), *The Culture of National Security: Norms and Identity in World Politics*, Columbia University Press, New York, 1996, apud Michael Barnett and Raymond Duvall, "Power in International Politics", in *International Organization* No. 59, Winter 2005, pp. 39-75, p. 41, DOI: 10+10170S0020818305050010, accessed on 12.10.2020.
[5] Michael Barnett and Raymond Duvall, *op. cit.*, p. 41.
[6] *Ibidem*, p. 40.
[7] *Ibidem*, p. 43.
[8] *Ibidem*, pp. 42-43.
[9] *Idem*.
[10] *Idem*.
[11] Colin S. Gray, *Hard Power and Soft Power: the Utility of Military Force as an Instrument of Policy in the 21st Century*, SSI Monograph, 2011, p. 5, URL: https://issat.dcaf.ch/Learn/Resource-Library2/Policy-and-Research-Papers/Hard-Power-and-Soft-Power-The-Utility-of-Military-Force-as-an-Instrument-of-Policy-in-the-21st-Century, accessed on 11.10.2020.

as values, ideas, culture, institutions, etc.[12] It refers to the power of persuasion using the mentioned intangibles in order to achieve the foreign policy goals[13]. Nye does not deny the importance of hard power, but argues that power depends upon context that, in our days, is like a "three-dimensional chess game": the military power is on the top board and is unipolar; the economic relations are the on the middle board that is multipolar, and transnational relations, with respect to climate change, illegal drugs, and terrorism, are on the bottom board where power is chaotically distributed[14]. In this contemporary context, there is a need for "a progressive realist policy" that stresses the importance of combining "hard military power" with "soft attractive power" into "smart power of the sort that won the Cold War"[15]. Nye argues that smart power is about developing both an integrated strategy based on resources and a tool kit to achieve national objectives based on hard and soft power[16]. What makes them smart power is the moral posture that attracts others even if that state actor will continue to rely on its economic and military power[17]. His analysis is referring to USA prior to Trump Administration and COVID-19 pandemic. One might argue that this power of attraction is even more useful now, once the pandemic is expanding, but the question that arises is if the health system resources, so needed in managing the pandemic, are used as source of power that is setting the international relations of contemporary world? Are they a source for soft or hard power? Are they to be used, in Nye's terms, as "power over others" or "power with others"?

The thematic literature mentions, mainly, six sources of states' power: national will, political capacity, wealth, geography, population, and natural resources[18]. As seen, there is no mention about health resources[19], not even in the case of wealth, that is defined traditionally in terms of GDP. All of the six sources are related in one way or another to state's capacity to win a war, even if they are not enough to ensure victory. Thus, national will is about the existence of a sense of purpose socially accepted that leads the public in sacrificing in the name of achieving the foreign policy goals. The political capacity is defined as state institutions' capacity to create and implement policy, to build a coherent agenda of foreign policy. Wealth, as seen above, is defined as total value of goods and services produced by one

[12] Joseph S. Nye Jr., "Hard, Soft, and Smart Power", in Andrew F. Cooper, Jorge Heine, and Ramesh Thakur (Eds.), *The Oxford Handbook of Modern Diplomacy*, 2013, DOI: 10.1093/oxfordhb/9780199588862.013.0031, accessed on 10.10.2020.
[13] Glenn P. Hastedt and William F. Felice, *Introduction to International Politics: Global Challenges and Policy Responses*, Rowman & Littlefield, Maryland, 2019.
[14] Joseph S. Nye, "Progressive Realism", in *The Bankok Post*, August 25, 2006, URL: https://www.belfercenter.org/publication/progressive-realism, accessed on 10.10.2020.
[15] *Idem*.
[16] Richard L. Armitage and Joseph S. Nye, Jr. (Cochairs), *CSIS Commission on Smart Power: a smarter, more secure America*, 2007, p. 7, URL: https://www.csis.org/analysis/smarter-more-secure-america, accessed on 11.10.2020.
[17] Pavlos Papadopoulos, "Joseph Nye: The world needs a stronger and more effective Europe", in *Ekathimerini*, 8 May 2020, URL: https://www.ekathimerini.com/252440/article/ekathimerini/comment/joseph-nye-the-world-needs-a-stronger-and-more-effective-europe, accessed on 11.10.2020.
[18] Glenn P. Hastedt and William F. Felice, *op. cit.*, 2019, pp. 133-138.
[19] A.N.: *Health resources* are defined by World Health Organization as consisting of "all organizations, people and actions whose primary intent is to promote, restore or maintain health. This includes efforts to influence determinants of health as well as more direct health-improving activities. A health system is therefore more than the pyramid of publicly owned facilities that deliver personal health services. It includes, for example, a mother caring for a sick child at home; private providers; behaviour change programmes; vector-control campaigns; health insurance organizations; occupational health and safety legislation. It includes inter-sectoral action by health staff, for example, encouraging the ministry of education to promote female education, a well-known determinant of better health" (*Everybody business: strengthening health systems to improve health outcomes: WHO's framework for action*, 2007, p. 2).

country's firms at home or abroad; a high GDP allows a country to build the necessary industrial and technological base for producing modern military weapons. Geography is closely linked to one state's definition and answer to national security threats, and population is the pool for military forces and a productive labor force. Finally, natural resources might both offer wealth, but also undermine one country's development efforts[20].

Returning to Nye's theory of soft power, it is important to stress out the idea of sources of power based on the basic power typology: the sources of soft power are culture, political values and foreign policy, and the sources of hard power are military and economic capabilities[21]. Soft power is used to co-opt (manipulate the opponents in order to attract them by one actor's side), to attract (using policy for attracting countries that share a similar vision), and to establish one's agenda. Hard power is used for inducements (foreign policy based on temptations and rewards, military or economic), coerce (sanctions and force), and command (results imposed by command).

In order to be able to validate the starting premise of this paper, the following section will focus on the way in which a pandemic affects the international relations and how IR theories approach it.

2. The way in which a pandemic affects the international relations. Case study: COVID-19 pandemic

One constant of our days is that almost no one is isolated anymore. This applies not only to information and transfer of goods, but also to pathogens. Global interconnectedness allows diseases to spread regardless of physical borders and areas of social life. This will also shape the international relations both in a positive and in a negative manner. The positive side of this change refers to the emergence of international cooperation in an attempt to tame and manage the pandemic. That is, in the above mentioned terms of Nye, "power with others". But the negative dimension of change refers to the competition for resources, especially health resources, triggered by various states, that is combined with a "competition" for finding the culprit and a rebirth of nationalism.

In the case of COVID-19 pandemic, the majority of state actors have opted for "power with others" approach[22], but there are some events and declarations that shows that Realist theory is still valid[23] and the power politics in not dead.

The latter is surprising since the Realist approach of international politics does not give attention to issues such as pandemics[24]. One of the most important representative of Realism, Stephen M. Walt, argue that this pandemic points out the fact that states are still the main actors in the global policy due to the fact that, in times of danger, people seek protection from the state, not from non-governmental organizations, multinational corporations or global

[20] *Idem*.
[21] Joseph S. Nye, Jr., *op. cit.*, 2013.
[22] See, for instance, the common EU response to COVID-19, the UN Comprehensive Response to COVID-19, and GAVI, the Vaccine Alliance (a coalition that is dedicated to equitable access to COVID-19 tests, treatments, and vaccines).
[23] A.N.: See the US statements regarding the withdrawal from the World Health Organization, the "passing of guilt" game between US and China, perspectives of creating and disseminating a vaccine based on spheres of influence and economic and politic resources, etc.
[24] Stephen M. Walt, "The Realist's Guide to the Coronavirus Outbreak", in *Foreign Policy*, 9 March 2020, URL: https://foreignpolicy.com/2020/03/09/coronavirus-economy-globalization-virus-icu-realism/, accessed on 12.10.2020.

markets[25]. Thereby, according to this approach, even if the global efforts are very important, states are still the most important actors.

It is obvious that COVID-19 pandemic is not only a health crisis, but a global one with a multidimensional impact over the international politics in the social, economic, and political area. In this context, the state is not only the most important actor, as realists argue, but the most affected actor by the pandemic. Unfortunately, Realism, even if it offers an excellent method of diagnosis, explaining the risks and dangers, does not offer any solutions for preventing such situations, as Seth A. Johnston argued in a reply to Walt's paper on Realism and pandemics[26]. He suggests Institutionalism as the best analytical solution for studying the way in which the current pandemic affects the international relations[27]. Institutionalism emphasizes the issue of self-interested cooperation and the importance of international organizations, but Realism explains better why state is the most important actor in maintaining order, why countries are competing for resources, and why there is a lack of trust in international organizations[28].

First of all, state proved to have the most important role in maintaining order during pandemic due to the measures taken: restricting the freedom of movement within it, managing health resources, closing national borders, etc. According to the International Monetary Fund (IMF) database, most EU countries have also closed non-essential sectors, including schools and restaurants[29]. Those measures helped in taming the pandemic at that time, even if not all of them were agreed initially by the World Health Organization (WHO).

Moreover, the Realist approach on international politics takes into account the competition for health resources such as medical masks, ventilators, treatment, and potential vaccines, even if its critics argue that this competition produces an inefficient allocation of resources[30]. But this does not mean that the competition does not exist, in Realist terms or not. For instance, a recent analysis of Duke Global Health Innovation Centre, GAVI, and World Bank shows that rich countries reserved half of projected COVID-19 vaccine supply[31].

Also, the Realist approach argues that there is a low level of trust in international organizations that seem to be unable to defeat the virus. The alternate points of view underline that international institutions are neither different solutions or nor competitors to state actions; furthermore, they are created by states in order to benefit from predictability, information, reduced costs, etc.[32] Still, reality shows that even powerful states do not always trust in international organizations such as WHO. For instance, US accused WHO for failure in sanctioning China, who is responsible for the pandemic. At the end of the second trimester of 2020, US contribution to WHO in the fight against pandemic was significantly reduced in comparison with other state or non-state actors (the 7th position with 34,189,300 USD)[33].

---

[25] *Idem*.
[26] Seth A. Johnston, "The Pandemic and the Limits of Realism. The foundational international relations theory has been revealed to be far less realistic that it claims", in *Foreign Policy*, 24 June 2020, URL: https://foreignpolicy.com/2020/06/24/coronavirus-pandemic-realism-limited-international-relations-theory/, accessed on 12.10.2020.
[27] *Idem*.
[28] *Idem*.
[29] ***, *Policy Responses to COVID-19*, 2020, International Monetary Fund, URL: https://www.imf.org/en/Topics/ imf-and-covid19/Policy-Responses-to-COVID-19#R, accessed on 20.06.2020.
[30] Seth A. Johnston, *op. cit.*, 2020.
[31] ***, "Rich countries grab half of projected COVID-19 vaccine supply", in *The Economist*, 12 November 2020, URL: https://www.economist.com/graphic-detail/2020/11/12/rich-countries-grab-half-of-projected-covid-19-vaccine-supply, accessed on 12.11.2020.
[32] *Idem*.
[33] ***, *WHO COVID-19 Preparedness and Response Progress Report - 1 February to 30 June 2020*, 2020, pp. 7-8, URL: https://www.who.int/publications/m/item/who-covid-19-preparedness-and-response-progress-report---1-february-to-30-june-2020/, accessed on 15.10.2020.

Moreover, the US decided to suspend its contribution to WHO and an official letter was sent by the US President to the Director-General of the WHO stating that, on 14th of April, 2020, he suspended the American contributions to the WHO[34]. Few months later, on 3rd of September, 2020, the Spokesperson for the US Department of State announced that the withdrawal from the WHO becomes effective on 6th of July, 2021 and by then the US will scale down its engagement with the Organization[35].

Credibility, trust and moral authority are important coordinates for power on international arena. If the international organizations have lost people's trust in them, according to realists, states are the actors that regain it. Since their response to the health crisis was not welcomed by a larger part of their citizens (see the social protests triggered by the lockdown measures and the rise of anti-vaccine movements) and the number of COVID-19 cases is still rising despite the efforts to manage the pandemic, one important step in this process seems to be winning the race for a vaccine. This is more than a desire to develop and implement a cure for the pandemic due to its obvious symbolism that is reminiscent of the space race: Russian Federation announced its vaccine called *Sputnik V*, as in the first artificial Earth satellite ever launched by the Soviet Union; the United States has called its programme *Operation Warp Speed*, with clear references to space and the popular TV series *Star Trek*[36]. In the same time, in the UK, AstraZeneca and the Oxford University are developing the *Oxford vaccine*. These are just some of the 48 candidate vaccines in clinical evaluation acknowledged by WHO[37], but their labels appear to bring into question two issues. One of them is the competition for power: the country that wins that race will enjoy great prestige and trust on the international arena that may set the *balance of power* for the future. The other one is *vaccine nationalism*: since the governments use to historical and nationalist names, there is an obvious inward approach and a possibility for signing agreements with pharmaceutical companies to supply their own populations with vaccines ahead of them becoming available for other countries (as *vaccine nationalism* is defined[38]). Related to the latter, but rather as a solution to the pandemic crisis, is *vaccine diplomacy*[39], that prevents the negative effects of vaccine nationalism and ensures that there are no discriminations between countries whether or not they are vaccine developers.

Those two concepts are to be used not only when analyzing the vaccine, but also for *medical supplies* in general. The paper "The Covid-19 Pandemic: 21st Century Approaches to Tracking Trade Policy Responses in Real-Time" offers interesting data on the issue of changes in trade policy towards export and imports of medical products related to the COVID-19 pandemic: 85 jurisdictions have placed export restrictions on medical supplies since January 2020 until October 2020[40]. For instance, on 10th of April, 2020 the US Federal

[34] ***, *The Letter of the US President, Mr. Donald Trump, to His Excellency Dr. Tedros Adhanom Ghebreyesus, Director-General of the WHO*, 2020, Washington, URL: https://www.whitehouse.gov/wp-content/uploads/2020/05/, accessed on 10.10.2020.

[35] ***, *Update on US Withdrawal from the World Health Organization*, 2020, Washington, URL: https://www.state.gov/update-on-u-s-withdrawal-from-the-world-health-organization/, accessed on 12.10.2020.

[36] Matthew Lynn, "The race to find Covid vaccine has become a global power struggle", in *The Spectator*, 10 September 2020, URL: https://www.spectator.co.uk/article/the-race-to-find-a-covid-vaccine-has-become-a-global-power-struggle, accessed on 15.10.2020.

[37] ***, *Draft landscape of COVID-19 candidate vaccines*, 12 November 2020, URL: https://www.who.int/publications/m/item/draft-landscape-of-covid-19-candidate-vaccines, accessed on 12.11.2020.

[38] Helen Ramscar, "Vaccine Nationalism in the Age of Coronavirus", in *RUSI Commentary*, 19 May 2020, URL: https://rusi.org/commentary/vaccine-nationalism-age-coronavirus, accessed on 15.10.2020.

[39] Helen Ramscar, "Vaccine Diplomacy in Phase 2 of the Covid-19 Crisis", in TippingPoint2020, 7 April 2020, URL: https://tippingpoint2020s.com/2020/04/07/vaccine-diplomacy-in-phase-2-of-the-covid-19-crisis/, accessed on 15.20.2020.

[40] ***, *The Covid-19 Pandemic: 21st Century Approaches to Tracking Trade Policy Responses in Real-Time*, The *Robert Schuman* Centre for *Advanced Studies, Global Trade Alert, and The World Bank Group, 2 May*

Emergency Management Agency (FEMA) published a temporary rule (120 days) banning exports of five types of personal protective equipment (PPE) from the US without its explicit approval. That memorandum set forth the "policy of the United States to prevent domestic brokers, distributors, and other intermediaries from diverting (these products) overseas" so as to "ensure that these scarce or threatened PPE materials remain in the United States for use in responding to the spread of COVID-19"[41]. In the same time, the following items were designated "scarce or threatened materials": N-95 respirator face masks, PPE surgical masks, PPE gloves, etc.[42] Moreover, a statement of the US President, Donald Trump, at the 75th Session of the UN General Assembly (September, 2020) brings into attention important elements that configure US position in international politics during COVID-19 pandemic: the actor to be sanctioned for triggering the pandemic is China; the world is seen as divided into friends/partners and China, and friends will benefit upon US altruism in distributing the vaccine; due to the fact that the health resources are crucial in managing the pandemic, US has a central role in this process as a result of possessing these resources[43]. In the same time, China initially blamed US for triggering the pandemic (US servicemembers visiting Wuhan)[44] and, later on, accused it for disseminating conspiracy theory about COVID-19 and for worsening the relations between the two countries[45]. In fact, since the relations between US and China have been broken for a long time, the pandemic seems to be just one more pretext for a struggle for status on international arena.

There are other states that introduced banes on export of medical supplies, such as Belgium (in April, introduced a ban on exports of certain pharmaceutical drugs to countries outside the European Economic Area), Bulgaria (has banned the export of disinfectants and protective clothing to third countries), Czech Republic (in March, introduced an export ban on all class FFP3 respirator face masks and hand sanitizers), France (expanded range of medicines banned from export by distributors, such as: antibiotics, painkillers, sedatives and muscle relaxants, as well as several drugs being tested as possible treatments for COVID-19, including Remdesivir, Hydroxychloroquine, Lopinavir and Ritonavir), Germany (in March, issued a an export licensing requirement on certain personal protective equipment, such as protective safety glasses, masks, gloves and garments as well as face shields and protective spectacles or visors), Hungary (in March, introduced a temporary export ban on hydroxychloroquine-sulphate and pharmaceutical drugs containing it), Norway (in March, introduced an export ban on pneumococcal vaccines arising from concerns about domestic shortages during the COVID-19 pandemic), United Kingdom (imposed a ban on the sale of PPE to countries outside of the EU), etc.[46]

It is obvious that health resources, especially the medical supplies and medicines, become an important element of defining a new type of balance of power, taking the place of

---

2020, URL: https://www.globaltradealert.org/reports/54, accessed on 10.10.2020; Helen Ramscar, *op. cit.*, 7 April 2020.

[41] ***, "GTA COVID Trade Barrier Data Sheet", in *The Covid-19 Pandemic: 21st Century Approaches to Tracking Trade Policy Responses in Real-Time, 2 May 2020.*

[42] *Idem*.

[43] ***, *The Statement of the US President at the Seventy-fifth Session of the UN General Assembly*, 2020, Washington, URL: https://estatements.unmeetings.org/estatements/10.0010/20200922/cVOfMr0rKnhR/cJHrXk2KdRU8_en.pdf/, accessed on 15.10.2020.

[44] Lisa Winter, "Chinese Officials Blame US Army for Coronavirus", in *The Scientist*, 13 March 2020, URL: https://www.the-scientist.com/news-opinion/chinese-officials-blame-us-army-for-coronavirus-67267, accessed on 15.10.2020.

[45] ***, "Coronavirus: China accuses US of spreading conspiracy theory", in *BBC News*, 24 May 2020, URL: https://www.bbc.com/news/world-asia-china-52790634, accessed on 15.10.2020.

[46] ***, "GTA COVID Trade Barrier Data Sheet", in *The Covid-19 Pandemic: 21st Century Approaches to Tracking Trade Policy Responses in Real-Time, 2 May 2020.*

an armaments race or the competitive acquisition of territory (as stated by the classic definition of *balance of power*), in this health crisis.

Beyond the Realist or Institutionalist approach on COVID-19 pandemic, there is still the important issue of its impact on people and society, economy, environment, domestic politics, military, and international relations. Since each and every above mentioned domain is negatively impacted and it is triggered a chain reaction among them, the military field will probably expect cuts to military budgets caused by economic austerity measures. This could mean that the most important resources that needs to be developed further, the health resources, could be and need to be defined as sources of power. The question that arises is whether they are a source or soft, hard, or smart power? Since the options of a great power's foreign policy (the US) seems to be on the one hand, inducements, if using them for helping the friends/partners (mainly to attract them on a side opposed to China) and, on the other hand, coerce, if not using them for helping the enemy, the answer is that, according to Nye's theoretical framework, the health system related resources tend to be used as a source of hard power[47].

Conclusions

Are or are not the health resources used as sources of hard power as the world struggles to manage one of the worst health crises of the last century?

If we stick to the classic Realist approach, the answer is no, since hard power is about maximizing one state's influence in the world by using military and economic resources.

Still, we must consider not only the type of sources and resources, but the spectrum of power behaviors in order to achieve the foreign policy goals, as neorealists argue. In this respect, the recent events show how health resources are used to both influence other actors by inducements and to coerce the actor identified as the enemy (in this case, perceived as the source of the pandemic).

The COVID-19 pandemic reveals two trends in international politics: on the one hand, the boost of international cooperation in order to manage the health crisis and the emergence of a so-called vaccine diplomacy, and, on the other hand, an inward approach that prompts nationalism. The latter brings into attention issues such as competition for medical supplies and health resources, race for vaccine, and vaccine nationalism. Those trends are possible frameworks for developing a new source of power (health resources, especially medical supplies) and a new type of coercion based on access to health resources. Thereby, the health resources will join the important resources specific to the Realist and Neorealist approaches of power.

At this point, it is not possible to say whether this evolution will be maintained, but if COVID-19 is just one of a new series of pandemics, it is possible that health resources will retain their role as sources of hard power.

BIBLIOGRAPHY:

1. ***, "Coronavirus: China accuses US of spreading conspiracy theory", in *BBC News*, 24 May 2020, URL: https://www.bbc.com/news/world-asia-china-52790634
2. ***, *Draft landscape of COVID-19 candidate vaccines*, 12 November 2020, URL: https://www.who.int/publications/m/item/draft-landscape-of-covid-19-candidate-vaccines

[47] A.N.: This assertion is further developed in "The New Power Politics, Network Analysis, and the COVID-19 Pandemic", in Lukasz Jurenczyk, Jaroslaw Mokrzycki, Robert Reczkowski (eds.), *International Research Conference GlobState III. Principles of War and Operational Art in the Context of the Future Security Environment: Central and East European Perspective*, Bydgoszcz, 2020, pp. 49-62.

3. ***, *Policy Responses to COVID-19*, 2020, International Monetary Fund, URL: https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19#R
4. ***, "Rich countries grab half of projected COVID-19 vaccine supply", in *The Economist*, 12 November 2020, URL: https://www.economist.com/graphic-detail/2020/11/12/rich-countries-grab-half-of-projected-covid-19-vaccine-supply
5. ***, *The Covid-19 Pandemic: 21st Century Approaches to Tracking Trade Policy Responses in Real-Time*, The Robert Schuman Centre for Advanced Studies, Global Trade Alert, and The World Bank Group, 2 May 2020, URL: https://www.globaltradealert.org/reports/54
6. ***, *The Letter of the US President, Mr. Donald Trump, to His Excellency Dr. Tedros Adhanom Ghebreyesus, Director-General of the WHO*, 2020, Washington, URL: https://www.whitehouse.gov/wp-content/uploads/2020/05
7. ***, *The Statement of the US President at the Seventy-fifth Session of the UN General Assembly*, 2020, Washington, URL: https://estatements.unmeetings.org/estatements/10.0010/20200922/ cVOfMr0rKnhR/cJHrXk2KdRU8_en.pdf
8. ***, *Update on US Withdrawal from the World Health Organization*, 2020, Washington, URL: https://www.state.gov/update-on-u-s-withdrawal-from-the-world-health-organization
9. ***, *WHO COVID-19 Preparedness and Response Progress Report - 1 February to 30 June 2020*, 2020, URL: https://www.who.int/publications/m/item/who-covid-19-preparedness-and-response-progress-report---1-february-to-30-june-2020
10. ARMITAGE, Richard L.; NYE, Joseph S. (Cochairs), *CSIS Commission on Smart Power: a smarter, more secure America*, 2007, URL: https://www.csis.org/analysis/smarter-more-secure-america
11. BARNETT, Michael; DUVALL, Raymond, "Power in International Politics", in *International Organization*, No. 59, Winter 2005.
12. CARLSNAES, Walter; RISSE, Thomas; SIMMONS, Beth A. (Eds.), *Handbook of International Relations*, SAGE Publications, 2013.
13. COOPER, Andrew F.; HEINE, Jorge; THAKUR, Ramesh (Eds.), *The Oxford Handbook of Modern Diplomacy*, 2013, DOI: 10.1093/oxfordhb/9780199588862.013.0031
14. GRAY, Colin S., *Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century*, SSI Monograph, 2011, URL: https://issat.dcaf.ch/Learn/Resource-Library2/Policy-and-Research-Papers/Hard-Power-and-Soft-Power-The-Utility-of-Military-Force-as-an-Instrument-of-Policy-in-the-21st-Century
15. HASTEDT, Glenn P.; FELICE, William F., *Introduction to International Politics: Global Challenges and Policy Responses*, Rowman & Littlefield, Maryland, 2019.
16. JOHNSTON, Seth A., "The Pandemic and the Limits of Realism. The foundational international relations theory has been revealed to be far less realistic that it claims", in *Foreign Policy*, 24 June 2020, URL: https://foreignpolicy.com/2020/06/24/coronavirus-pandemic-realism-limited-international-relations-theory
17. KEOHANE, Robert; MARTIN, Lisa, "The Promise of Institutionalist Theory", in *International Organization*, No. 20 (1)/1995, pp. 39-51, DOI: 10.2307/2539214
18. LYNN, Matthew, "The race to find Covid vaccine has become a global power struggle", in The Spectator, 10 September 2020, URL: https://www.spectator.co.uk/article/the-race-to-find-a-covid-vaccine-has-become-a-global-power-struggle
19. McGLINCHEY, Stephen; WALTERS, Rosie; SCHEINPLFUG, Christian (Eds.), *International Relations Theory*, E-International Relations, Bristol, 2017.
20. NYE, Joseph S., "Progressive Realism", in *The Bankok Post*, August 25, 2006, URL: https://www.belfercenter.org/publication/progressive-realism
21. PAPADOPOULOS, Pavlos, "Joseph Nye: The world needs a stronger and more effective Europe", in Ekathimerini, 8 May 2020, URL: https://www.ekathimerini.com/252440/article/ekathimerini/comment/joseph-nye-the-world-needs-a-stronger-and-more-effective-europe
22. RAMSCAR, Helen, "Vaccine Diplomacy in Phase 2 of the Covid-19 Crisis", in *TippingPoint2020*, 7 April 2020, URL: https://tippingpoint2020s.com/2020/04/07/vaccine-diplomacy-in-phase-2-of-the-covid-19-crisis

23. RAMSCAR, Helen, "Vaccine Nationalism in the Age of Coronavirus", in *RUSI Commentary*, 19 May 2020, URL: https://rusi.org/commentary/vaccine-nationalism-age-coronavirus.
24. VASQUEZ, John A., *The Power of Power Politics. From Classical Realism to Neotraditionalism*, Cambridge University Press, 2004.
25. WALT, Stephen M., "The Realist Guide to the Coronavirus Outbreak", in *Foreign Policy*, 9 March 2020, URL: https://foreignpolicy.com/2020/03/09/coronavirus-economy-globalization-virus-icu-realism.
26. WINTER, Lisa, "Chinese Officials Blame US Army for Coronavirus", in *The Scientist*, 13 March 2020, URL: https://www.the-scientist.com/news-opinion/chinese-officials-blame-us-army-for-coronavirus-67267

COVID-19: PROPAGANDA AND THE FEAR-FACTOR IN THE INTERNATIONAL AGENDA – A PERSONAL EXPERIENCE

Maia URUSHADZE, Ph.D.
Political Science Researcher, Caucasus International University, Tbilisi, Georgia.
E-mail: maya.urushadze@gmail.com

Abstract: *At the start of 2019, when humanity was not yet sharply facing the threat of COVID, the security paradigm showed a tendency to change. In particular, in recent years, as far back as the beginning of last year, the attention of security experts has been focused on qualitatively new challenges. It is natural that COVID-19 pandemic has already changed the safety requirements of the world. Societies have changed in each country, in particular human relations, culture, and rules. The domestic and foreign policies of the states, border regulations, and the specifics of transportation have also changed. Besides, the most important social factor can be considered that a new struggle of interpretations has been activated in the media agenda. The worldwide international media agenda observation reveals that there are a lot of conspiracy theories have been developed around the pandemic virus, which strengthens mainstream ideological narratives through the fear factor. They have appealed to the fears in two conflicting directions and developed relevant interpretations in societies globally, within states. In this power struggle of interpretations, it is seen that the pandemic has imposed new responsibilities on the ruling elites, but also gives visible advantages to all local authorities. In particular, it is in their hands that the powerful, fear-backed levers of management are accumulated, with the help of which it is possible to strengthen the power. In the article is given the case of author's personal experience.*

Keywords: *Covid-19; new security paradigm; conspiracy theory; global affairs; fear-factor.*

Introduction: COVID-19 and the New Security Paradigm

At the start of 2019, when humanity was not yet sharply facing the threat of COVID, the security paradigm showed a tendency to change. In particular, in recent years, as far back as the beginning of last year, the attention of security experts has been focused on qualitatively new challenges.

"The nature, scope and spectrum of conflicts and security are changing. The emerging security paradigm is framed by new asymmetrical warfare, increasingly easy access to increasingly powerful weapons, violent extremism, conflicting motivations, and a relatively chaotic organisation of the parties involved. The diversification of threats and actors is generating new challenges to the defence and security communities, as well as to society as a whole."[1] – it is said on the official website of the European Commission.

[1] ***, *Knowledge for policy: Indicators of significance to changing security paradigm*, European Commission, 2020, URL: https://ec.europa.eu/knowledge4policy/foresight/topic/changing-security-paradigm/indicators-significance-changing-security-paradigm_en

In a report on World Sustainability for 2019 prepared by the Peace Foundation[2], fragile states index was reflected as follows:

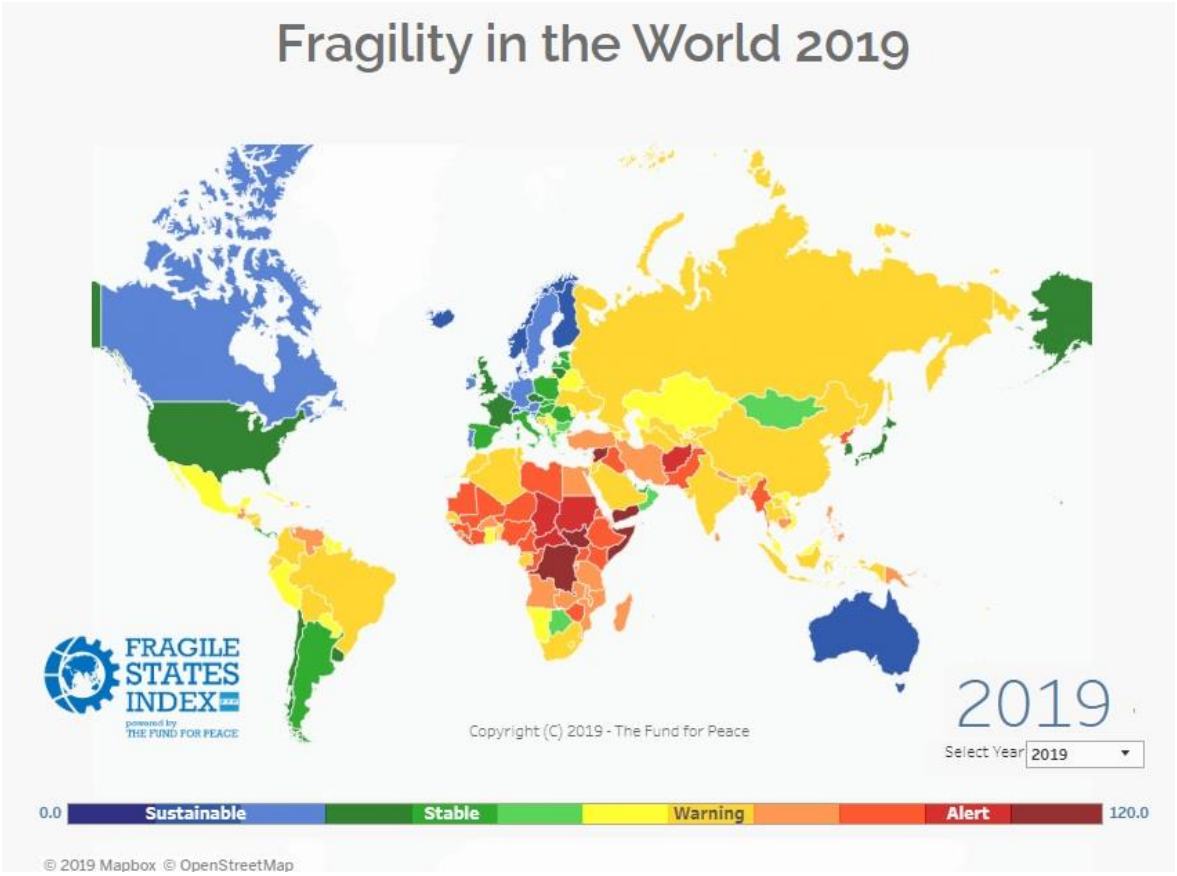


Figure no. 1. Fragile States Index – Fragility in the World, European Commission, 2020, Knowledge for policy: Indicators of significance to changing security paradigm[3]

It was a signal to the international community to start looking for new security formats and tools. It would be superfluous to say that the security paradigm is substantially unchanged since the security factor is more important than other social factors. The need for security, in a broad sense, outweighs the physical needs. Even the instinct of self-preservation is to respond to a threat, in some cases -subconsciously, and in some cases - directly reflect on the threat of destruction.

Therefore, it is natural that COVID-19 pandemic has already changed the safety requirements of the world. Societies have changed in each country, in particular human relations, culture, and rules. The domestic and foreign policies of the states, border regulations, and the specifics of transportation have also changed. Besides, the most important

[2] A.N.: There in the study were used 4 main indicators as indicators to assess the stability of individual countries: cohesion, economic, political and social, including the cross-cutting factors. Each indicator was broken down into 3 components and analyzed: in terms of cohesion – for security apparatus, factionalized elites and group grievance; In terms of economic factors – for economic decline, uneven economic development and human flight/brain drain; In terms of political factors – for state legitimacy, public services, human rights and rule of law; In terms of social factors - for demographic pressures, IDPs and internally displaced persons, and in terms of cross-cutting factors - for external intervention. URL: https://fragilestatesindex.org/ -

[3] Source: https://ec.europa.eu/knowledge4policy/foresight/topic/changing-security-paradigm/indicators-significance-changing-security-paradigm_en

social factor can be considered that a new struggle of interpretations has been activated in the media agenda.

The ideological differences in adherence to social distancing are shown in data from two MTurk studies with U.S. respondents (total N =1,153) which revealed an ideological divide in adherence to social distancing guidelines during the COVID-19 pandemic. Specifically, political conservatism inversely predicted compliance with behaviors aimed at preventing the spread of the COVID-19. Differences in reported social distancing were mediated by divergent perceptions of the health risk posed by COVID-19 (Studies 1 and 2), which were explained by differences in self-reported knowledge of COVID-19 (Study 1) and perceived media accuracy in covering the pandemic (Studies 1 and 2).[4]

"The politicization of COVID-19 may have prompted conservatives to discount mainstream media reports of the severity of the virus, leading them to downplay its health risks and consequently adherence less to social distancing protocols. These effects hold when controlling for key demographic characteristics as well as psychological variables, including belief in science and COVID-19-related anxiety. Thus, political ideology may uniquely explain COVID-19 behavior."[5]

1. Conspiracy theories and fear

The worldwide international media agenda observation reveals that there are a lot of conspiracy theories which have been developed around the pandemic virus, strengthening the mainstream ideological narratives through the fear factor. They have appealed to the fears in two conflicting directions and developed relevant interpretations in societies globally, within states.

Namely, these areas are (a) fear of the virus itself and (b) fear of the limitations dictated by the danger of that virus. As for the third interpretation, which combines the two and introduces total nihilism, we will talk about a little later.

Undoubtedly, the leading theory among conspiracy ones is that "this virus was created artificially to reduce the number of human beings" and that "its creators had the vaccine in their hands from the very beginning". These interpretations contain various theories about the probable creators of the virus, including the "influential globalists", the "narrow circle of magnates", the "Masonic lodge", etc. However, the interpretation of the virus of "Chinese origin" undoubtedly leads here, according to which in the pre-pandemic period "China, with her ambitious geopolitical interests, took active action and created biological weapons against the rest of humanity." These ideas of conspiracy theory have one thing in common: each of them views the virus as a dangerous biological weapon, which adds irrational fears to the natural caution, and this way, they serve or assist the different ideological camps, including opposing camp to impose additional restrictive regulations due to pandemics.

The talk of politicising the pandemic and turning it into an ideological one began in the very first decade of 2020. In the context of US-China relations, The Begin-Sadat Center for Strategic Studies (also known by its acronym, the BESA Center) analyst Emil Avdaliani wrote that the last element of several components to the growing US-China rivalry— a clear ideological separation – was lacking, but is now rapidly evolving as a result of coronavirus: "The coronavirus pandemic is becoming a battle of narratives. Ultimately, the question of

[4] Hank Rothgerber, Thomas L. Wilson, Daniel L. Rosenfeld, et.al, "Politicizing the COVID-19 Pandemic: Ideological Differences in Adherence to Social Distancing", April 2020, URL: https://www.researchgate.net/publication/340850359_Politicizing_the_COVID19_Pandemic_Ideological_Differences_in_Adherence_to_Social_Distancing

[5] *Ibidem.*

whether the virus's spread was a product of human action or an accident might not matter very much. Whatever its origin, the pandemic has highlighted wide ideological differences between the democratic West and non-democratic China. On a broader level, the democratic West now stands more starkly in opposition to non-democratic Asia."[6]

Numerous interpretations are found among theories that reinforce fears about the limitations dictated by the danger of the virus. Among them are "the virus is normal", "it is no different from seasonal flu", "it is a conspiracy of pharmaceutical companies" and "fears are artificially allayed". Undoubtedly, the leading interpretation here is that the threat of a pandemic is done in order to subjugate societies, to gain leverage over them.

The content distribution of interpretations is also wide on the media agenda. The media, whose editorial policies are loyal to the ruling political force, are widely using agenda-setting and framing to focus on the credibility of anti-epidemic measures, the accuracy of testing, the necessary strict adherence to necessary restrictions, and the fault of the disobedient part of the public through the spread of the epidemic. At the same time, those media outlets whose editorial policies are loyal to opposition political forces focus on the weakness of government measures, the unreliability of testing, the ineffectiveness of additional restrictions, and the use of these restrictions for unscrupulous, political purposes.

Numerous interpretations are found among the theories that reinforce the fear of limitations caused by the danger of the virus. These include "the virus is normal", "it is no different from seasonal flu", "this is a conspiracy of pharmaceutical companies" and "fears are artificially dispelled". Undoubtedly, the leading interpretation here is that the threat of a pandemic is carried out in order to subjugate societies in order to gain leverage over them.

Undoubtedly, in this power struggle of interpretations, it is seen that the pandemic gives visible advantages to all local authorities. In particular, it is in their hands that the powerful, fear-backed levers of management are accumulated, with the help of which it is possible to strengthen the power. The pandemic has imposed new responsibilities on the ruling elites, however, the situation created by the pandemic in the world is favorable for the authorities and, naturally, effective managers don't miss this "bonus".

2. COVID influence on global affairs

In this regard, there are examples of countries where authorities have refused to restrict personal freedoms due to a pandemic. The struggle of interpretations on the example of these countries has intensified in two ideological contexts: the rightists against the leftists and the globalists against the anti-globalists. In particular, it turned out that on the one hand, these authorities made a decision characteristic of liberal ideology and rejected restrictions on freedoms in favor of the economy and development. But, on the other hand, on the example of these countries, the statists reprimand the authorities that they, out of respect for personal freedoms, shifted the burden of defending themselves from the threat of a pandemic to the high responsibility of the population, resulting in high casualties. The basis for their view is statistics, which show that in countries where the pandemic was not regulated by strict regulations, health systems could not withstand the high pressure, and the first wave of the virus resulted in high casualties. However, final figures are not yet visible to show if it has prepared these countries for the second wave of the virus and how liberal policies will affect the final consequences of the pandemic for these countries.

Due to the pandemic, the struggle of interpretations intensified in the camps of the proponents and opponents of globalization as well. In particular, the fear factor for the threat

[6] Avdaliani, E., "The Battle of the Coronavirus Narratives", *BESA Center Perspectives*, Paper No. 1, 564, 2020, URL: https://besacenter.org/perspectives-papers/coronavirus-narratives/

of COVID widespread on the one hand has strengthened the frame of 'common effort against the threats facing humanity', which is one of the important ideological pillars of the proponents of globalization. On the other hand, the same fear factor has intensified the need for states to close borders, control foreign trade with additional regulations, and thus prevent the internal spread of the pandemic. This fear is conducive to forces with anti-globalist ideas and supporters of nation-state ideology.

Of course, in a pandemic situation, the need for crisis management has increased in most countries of the world. Constantly changing regulations and the instability of international traffic have damaged international agreements and put many sectors of the economy in a force majeure situation. Among them - tourism and international traffic between countries. In many cases, the force majeure situation has relieved many responsibilities of both government and commercial entities, but on the other hand, due to the same disorder, there are more cases in the world when governments and commercial structures use this situation as an additional tool to strengthen their position or avoid financial responsibility.

3. Personal experience – A case study

An example is a case that happened to me at the end of August this year. On August 27, 2020, at Minsk airport, I was deprived of the opportunity to use the transit area during an international flight from Tbilisi to Warsaw. In fact, Warsaw launched new COVID-regulations on August 27th, right a few minutes before my flight had taken off, but even according to the new rules[7], for me – Ph.D. researcher with documentary approved connections to the respectful research institutions – there were no restrictions to enter the country. But the flight operator, BELAVIA – Belarusian Airlines permit to go through the "green corridor" just people with Polish citizenship or a permanent residence in Poland. So, I was required to "go to the transfer through the first floor," through the passport control via Minsk International Airport. I tried to get the right to pass to the transit area several times, I approached the desk a few times and tried to show my documents but all times I was shown to exit through the "first floor", to go through passport control.

In the first view, it was not a huge problem, but really, it was. First, at that moment I was traveling from Georgia – "Green zone" (at that moment and not Poland nor other EU countries were not requiring any additional documents to enter the country). But I knew: Belarus was on the 'red list' for Poland due to the new COVID rules, so entering from Minsk in some European countries (including Poland), according to constantly updated COVID regulations, at that time was allowed only after a mandatory two-week length quarantine.

Secondly, after entering Minsk I faced an increased risk of COVID infection.

Lastly, the reason for my voyage was that I was sent on a short-term scientific visit to Warsaw, and a week later to Bucharest, and my visit was financed by the State Science Foundation of Georgia. My research visit was previously planned and there were no possibilities to change my budget. That's why I was not able to change my presence length in Warsaw, as well as I was not able to change my flight to Romania from Poland planned on the 8th day of my visit and my flight back (Bucharest-Warsaw-Tbilisi) on the 15th day. Thatswas why I had reserved all non-refundable residences in both cities, so I was not able to change the dates too. I had planned meetings in both countries and I had to work hard even at the Minsk airport while waiting for a transfer.

[7] ***, "Coronavirus: information and recommendations", URL: https://www.gov.pl/web/coronavirus/travel

After that, it should have been printed there on the airport surveillance cameras how they removed me from boarding the Warsaw flight, how humiliatingly they took my passport away and took me out of the boarding hall.

After my flight departed, I got the opportunity to communicate with BELAVIA staff and, after reviewing my documents, I was told that "my documents were not appropriate" and "Warsaw would not let me in even if I would have not entered Minsk", which is not true. The Polish Embassy can confirm that the problem arose only after I was not allowed through the transit corridor in Minsk and the Minsk stamp appeared in my passport. Even after that, my visit, fully funded by the National Science Foundation, might not be disrupted, but only delayed for 2 weeks, and require additional costs for mandatory quarantine. The problem was that I didn't have free funds for a single decision on making additional expenses to the budget of the visit.

As a way out of the created situation, BELAVIA offered me the closest flight to Berlin or Amsterdam, from where I could myself get to Warsaw or Bucharest by train or bus, evading passport control, but this way was unacceptable for international security and ethical reasons. Ultimately, after urgent multilateral telephone and letter communications with the consulates of Georgia in Belarus, Poland, and Bucharest, as well as with the Foundation and the hosts in Warsaw and Bucharest, the optimal outcome was my return to Georgia and the passage of mandatory quarantine upon returning home from the zone of the high risk of infection, after which I would be confident in the safety and expediency of a repeat visit to Poland and Romania. So, BELAVIA provided me with a ticket just to Istanbul.

In total, the uncoverable direct damage to the scientific project was not huge, but after the incident I got infected by COVID, this incident violated the terms for defending my dissertation, and most importantly, this incident violated the timeline and budget of a scientific project with a total cost of 12,000 Euro.

Taking into account the constantly and dynamically changing situation in the field of regulations created in the world in connection with the spread of COVID infection, as well as the ambiguous political situation created at the time of my transit in Belarus itself, I enter the position of BELAVIA employees, who constantly have to work in a tense setting. Therefore, I asked the decision-makers at BELAVIA to compensate as soon as possible only direct damage received to let me continue my urgent work and make interrupted visits. But, BELAVIA answered again the same, that they don't recognize their fault, 'because the decision was made by Poland' and 'my documents were not appropriate'.

Conclusions

Because of the background of my personal experience, the Pandemic situation can be viewed in a different context. The assumption relates to the political situation in Belarus at that moment was uncertain.

On the one hand, the Belarusian officials did not recognize COVID as a threat, and narratives most of them were aimed at reinforcing conspiracy theories that all the restrictions were due to the lockdown of the world economies and thus the intention to gain global control. For this reason, Belarus did not close its borders and introduced anti-pandemic rules in the country only superficially. During my two-day stay in Belarus, I was convinced that even the demand for the use of masks was considered a tiring whim by the public in this country, and thus the masses didn't defend this rule.

On the other hand, due to the frequent restrictions on human rights and freedom of speech in the country, there was a sharp political confrontation between the opposition and the government, while the government narratives mainly concerned external forces that

encouraged the opposition to be active against the government. Consequently, government forces were active in preventing external contacts, and at this time, it is natural to look with suspicion at the passengers of the exiled President of Georgia, Mikheil Saakashvili, the organizer of the "Rose Revolution" demonized by Russian propaganda. Especially since the main propagandistic narrative of the Russian media in the post-Soviet space was the threat of exporting "color revolutions". This may also explain the indifferent and rude attitude of BELAVIA staff that led to this incident. In this context, it is interesting to note that after the forced transfer of passengers on August 27 at the Minsk airport, on October 29-30 on social networks related to the events in Belarus briefly appeared the information that "the Belarusian authorities had found "Sonder groups" sent from Georgia to support protests against Lukashenko". However, this information disappeared very soon, and since 1st September is no longer sought in the comments.

However, this does not change the fact that BELAVIA indirectly blamed the COVID-restrictions on this case. That's why I immediately informed them that the incident occurred in Minsk will serve as a clear example of new challenges faced by the international community in frame of the struggle of interpretations, due to the fears about the danger of the spread of COVID infection on the one hand, and due to the need of international coordination of new anti-pandemic regulations – on the another.

BIBLIOGRAPHY:

1. ***, "Coronavirus: information and recommendations", URL: https://www.gov.pl/web/coronavirus/travel
2. ***, "Reopen EU", *EU*, URL: https://reopen.europa.eu/en/map/POL/2008
3. ***, *Knowledge for policy: Indicators of significance to changing security paradigm*, European Commission, 2020, URL: https://ec.europa.eu/knowledge4policy/foresight/topic/changing-security-paradigm/indicators-significance-changing-security-paradigm_en
4. AVDALIANI, E., "The Battle of the Coronavirus Narratives", *BESA Center Perspectives*, Paper No. 1, 564, 2020, URL: https://besacenter.org/perspectives-papers/coronavirus-narratives/
5. ROTHGERBER Hank, WILSON Thomas L., ROSENFELD Daniel L., et.al, "Politicizing the COVID-19 Pandemic: Ideological Differences in Adherence to Social Distancing", April 2020, URL: https://www.researchgate.net/publication/340850359_Politicizing_the_COVID19_Pandemic_Ideological_ Differences_in_Adherence_to_Social_Distancing

COVID-19 CRISIS – FRAGILE BALANCING BETWEEN CONTAINMENT MEASURES AND ECONOMIC GROWTH

Cristian BĂHNĂREANU, PhD.
Senior Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania.
E-mail: cristi.bahnareanu@gmail.com

Abstract: *In 2020, the COVID-19 pandemic, the worst health crisis in the last 50 years, has disturbed the society and the economy through a series of negative effects to the people health and economic growth. Measures to prevent and combat the spread of the virus taken by most countries in the world in March-April have led, particularly in the second quarter of this year, to a generalized decline in economic activity. In this context, the paper analyzes whether the national authorities in the affected countries have managed to find a proper balance between measures to protect the health of citizens and those to ensure the smooth running of the economy.*

Keywords: *COVID-19 pandemic; health crisis; containment measures; economic growth; balance.*

Introduction

The year 2020 began with another kind of crisis, which started by timidly knocking on the "door" of Western states. Since March, the SARS-CoV-2 coronavirus has spread rapidly in almost all countries, whether developed or underdeveloped ones, and the health and economico-social effects became more serious. National health systems have been slowly overwhelmed by the number of patients and cases of infection. In the last 50 years, mankind has never faced such major health problems since the Hong Kong Flu[1], so governments have had to pump significant human, financial and material resources into the health and economic system to cope with the COVID-19 pandemic and related problems.

After a period of calm in the summer months, the health crisis is again on an upward trend (the second wave of the pandemic). It has triggered other crises in the economic field (transport, tourism, hospitality, and the economy as a whole) and social dimension (degradation of the population's health, unemployment, protests against containment measures). Increasing government debt is a problem facing most states, especially on the European continent, where the officials in Brussels suspended the rules on budgetary discipline established by the Stability and Growth Pact at the end of March 2020.

In this respect, the paper briefly presents the dynamics of the COVID-19 crisis and its effects in the economic area, as well as the lockdown measures that have been imposed at the national level to prevent and combat the spread of the pandemic. Also, based on EU, OECD and Worldometer data, there will be analyzed the existence of a certain balance between the containment measures, the number of new coronavirus cases, and the rate of economic growth, particularly in second quarter of 2020.

[1] A.N.: According to UN, the most severe influenza pandemics in the last 100 years was the Spanish Flu with 20-50 million deaths in 1918-1919, Asian Flu with 1-4 million deaths in 1957-1958, and Hong Kong Flu with 1-4 million deaths in 1968 (***, *Past pandemics*, World Health Organization, URL: https://www.euro.who.int/en/health-topics/communicable-diseases/influenza/pandemic-influenza/past-pandemics, accessed on 10.09.2020).

1. The crisis triggered by the new coronavirus

SARS-CoV-2, a coronavirus that was first detected in late 2019 in Wuhan, Hubei Province, China, has rapidly spread globally in more than 215 countries and territories and infected more than 50 million people. In the nine months since the beginning of the pandemic[2]. The worst affected countries by the airborne transmission virus are: the US – over 245,000 deaths, Brazil – over 160,000, India – over 125,000, Mexico – over 95,000, the UK – almost 50,000, Italy, France and Spain – about 40,000 victims each[3]. In Romania, the coronavirus disease started on February 26, 2020 with a first case in Gorj[4] and now has reached over 300,000 cases with 8,000 deaths, most in Bucharest and Suceava County. The most vulnerable people to Covid-19 infection are the elderly who suffer from other medical conditions (diabetes, obesity, hypertension, ischemic heart disease, cerebrovascular disease or chronic kidney disease), most of the victims being over 60 years.

From the earliest stages of the health crisis, most affected countries declared state of emergency/necessity/alert and implement harsh measures to prevent and combat the spread of the virus (partial/complete lockdown): limiting the movement of people and physical distancing; hospitalization, institutionalized quarantine or isolation at home of infected persons and suspects; placing under quarantine of some localities or regions; partial/total closure of border crossing points, as well as tightening of border controls; reduction/suspension of certain categories of transport (air, rail, road, including public transport), except freight; reduction/cessation of economic activities by carrying out work from home or sending employees to technical unemployment; temporary closure of schools, shopping malls, hotels, casinos, clubs, restaurants, cafes and other public places, as well as sports and cultural centers; closure of parks, playgrounds and urban open spaces; suspension / cancellation of social activities with the participation of large masses of people, etc.[5] All these containment measures were accompanied by certain postponements/exemptions from taxes and duties, as well as financial compensations from the state for the categories of persons and economic sectors most affected by the imposed restrictions. Also, those who did not comply with the restrictions taken and quarantine were severely sanctioned, going as far as the opening of criminal cases.

Based on the lessons learned from the first phase of spring-summer pandemic crisis, the legislation in the field was reviewed, as well as a series of protocols, procedures, plans and strategies at national level, including Romania, to deal more promptly and efficiency in other such situations. Stocks of medical materials and equipment have been replenished, medical staff, hospitals and quarantine areas were prepared for rapid response, the role and missions of national institutions with responsibilities in the area[6] were strengthened for a better capacity for action and efficiency in decision-making and application of the necessary measures.

---

[2] On 11 March 2020, World Health Organization declares the coronavirus outbreak a pandemic (***, *WHO Director-General's opening remarks at the media briefing on COVID-19*, WHO, 11 March 2020, URL: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, accessed on 15.09.2020).

[3] ***, *COVID-19 Coronavirus Pandemic*, Worldometer, 2020, URL: https://www.worldometers.info/coronavirus, accessed on 15.09.2020.

[4] ***, "Primul caz de coronavirus în România", *Digi24*, 26 February 2020, URL: https://www.digi24.ro/stiri/actualitate/primul-caz-de-coronavirus-in-romania-1266806, accessed on 17.09.2020.

[5] Cristian Băhnăreanu, "The Economic Impact of COVID-19 Pandemic at the Beginning of 2020", *Strategic Impact*, No. 2/2020, Centre for Defence and Security Strategic Studies, "Carol I" National Defence University Publishing House, Bucharest, 2020, p. 103.

[6] In Romania, the institutions responsible for managing health crisis are the National Committee for Emergency Situations, the Ministry of Internal Affairs, the Ministry of Health, the Ministry of National Defence, etc.

Internationally, the World Health Organization, together with the European Union, NATO and other regional organizations (Red Cross, Médecins Sans Frontières), have developed a set of key objectives in order to increase cohesion, information exchange and the capacity and capabilities of response to such crises.

2. Economic effects of the health crisis

The first priority of the national authorities was to prevent and combat the spread of the new coronavirus and associated disease in order to reduce infection rates and pressure on health systems and then to resume economic activities and increase resilience to epidemics. In April 2020, half of the world's population was subjected to partial or total lockdown measures[7], as a result of extensive restrictions on people movement and economic and social activities applied by most states since the beginning of the health crisis. Although, in the short term, there have been a number of positive effects – decongestion of road traffic, reduction of air pollution and carbon emissions, decline in crude oil prices, decrease in the incidence of seasonal diseases, increase in population savings, crime reduction, development of digital capabilities, explosion of online commerce and courier services[8] –, the negative ones are much more and more serious because they affect large masses of people, professional categories, sectors of activity, the entire economy and society.

Probably the most important effect of the COVID-19 pandemic is the economic one, starting from the cessation of some economic activities and sectors and ending with the rapid increase of the public debts of the affected countries. Indeed, the world economy is facing the worst recession since the diplomatic crisis of July 1914 (-6.7%), the Great Depression of the 1930s (-17.6%) and the post-World War II period (-15.4%)[9], with a decline in GDP that could reach -4.36% in 2020[10] and an explosion of unemployment in many developed and less developed countries. In the absence of a viable vaccine, the losses to the world economy could reach 17.3 trillion dollars in the current year and, cumulatively, 35.3 trillion dollars in the next five years[11].

Since March 2020, the world's major economic powers – the US, China, Japan, Germany, India – have experienced the effects of the COVD-19 pandemic (as can be seen in figure no. 1), the initial shock causing major disruptions in global trade, transport and tourism, stress on financial markets and a sharp decline in commodity prices. The deterioration of most macroeconomic indicators has led to a strong setback in the world economy and growing fears of entering a recession. Measures taken to combat pandemic have disrupted production, created shocks on supply chain and difficulties in securing stocks of basic necessities. Reduced demand for goods and services, decreasing productivity and employment, declining incomes and profits

[7] Alasdair Sandford, „Coronavirus: Half of humanity now on lockdown as 90 countries call for confinement", *Euronews*, 3 April 2020, URL: https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou, accessed on 23.09.2020.
[8] Mauricio Cárdenas, "Looking at the Bright Side: 10 Positive Effects of the Pandemic", *Americas Quarterly*, 13 July 2020, URL: https://www.americasquarterly.org/article/looking-at-the-bright-side-10-positive-effects-of-the-pandemic, accessed on 23.09.2020; Cristian Băhnăreanu, *op. cit.*, 2020.
[9] Ayhan Kose, Naotaka Sugawara, „Understanding the depth of the 2020 global recession in 5 charts", *World Bank Blogs*, 15 June 2020, URL: https://blogs.worldbank.org/opendata/understanding-depth-2020-global-recession-5-charts, accessed on 25.09.2020.
[10] ***, *World Economic Outlook: A Long and Difficult Ascent*, International Monetary Fund, Washington, DC, October 2020, p. 8.
[11] Warwick McKibbin, Roshen Fernando, *Global macroeconomic scenarios of the COVID-19 pandemic*, CAMA Working Paper 62/2020, Australian National University, June 2020, p. 34.

have led to the loss of a significant number of jobs, which has strongly fueled the unemployment rate[12].

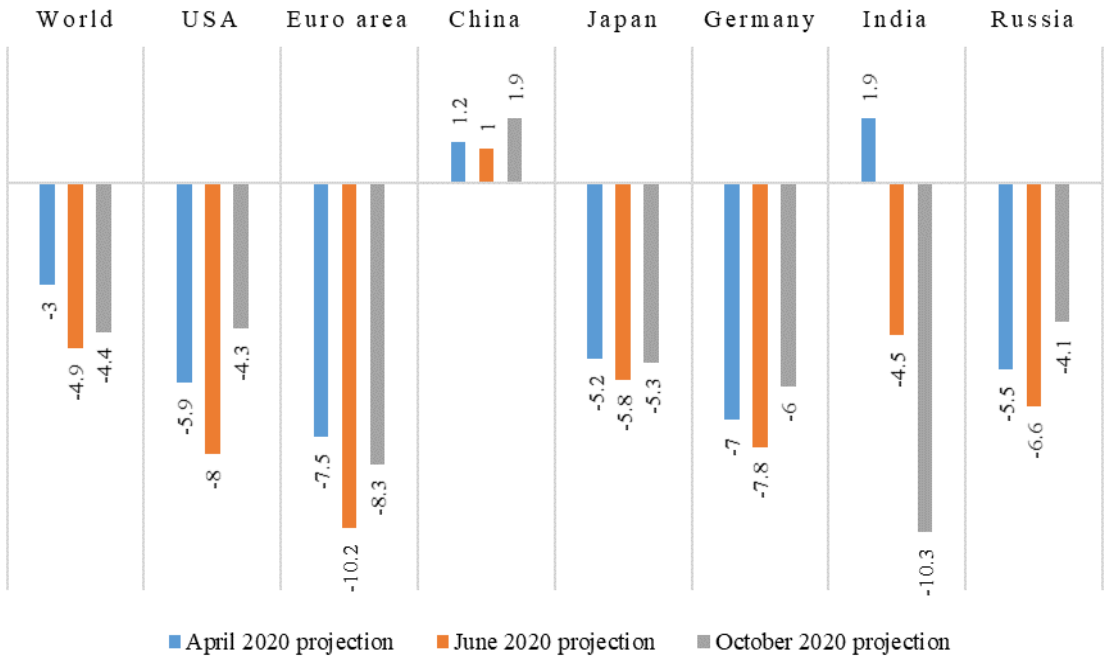


Figure no. 1: Projection of economic growth for 2020[13]

The economic problems in developed countries have spread rapidly to emerging markets and developing economies, with capital and trade flows falling sharply. The economic downturn generated by the pandemic and the high level of uncertainty about economic policy in the US and the Euro area have led to a strong decline in investment in less developed countries in Europe and Central Asia. To all these were added internal shocks, sometimes much more destructive to economic activity than external ones. But it seems that the impact of the COVID-19 crisis on the economy of the East Asia and Pacific region will be greatly mitigated, given that the recovery of the Chinese economy has been faster than expected[14].

[12] ***, *World Economic Situation and Prospects as of mid-2020*, Department of Economic and Social Affairs, United Nations, New York, 2020; ***, *Global Economic Prospects*, A World Bank Group Flagship Report, Washington, DC, June 2020; ***, *World Economic Outlook Update: A Crisis Like No Other, An Uncertain Recovery*, International Monetary Fund, Washington, DC, June 2020.

[13] ***, *World Economic Outlook: The Great Lockdown*, International Monetary Fund, Washington, DC, April 2020, p. 7; ***, *World Economic Outlook Update: A Crisis Like No Other, An Uncertain Recovery*, International Monetary Fund, Washington, DC, June 2020, p. 7; ***, *World Economic Outlook: A Long and Difficult Ascent*, International Monetary Fund, Washington, DC, October 2020, p. 8.

[14] Anna Fifield, "China's economy bounces back more quickly than expected from coronavirus", *The Washington Post*, 16 July 2020, URL: https://www.washingtonpost.com/world/asia_pacific/chinas-economy-bounces-back-more-quickly-than-expected-from-coronavirus/2020/07/16/b4285da2-c67a-11ea-a825-8722004e4150_story.html, accessed on 25.09.2020.

3. Finding a balance between containment measures and economic growth

In March, an OECD study showed that a month of strict containment of economic and social activities was equivalent to a decrease in the annual GDP growth rate of around 2%[15]. If the shutdown was to be extended for a period of about three months, this would certainly lead to a reduction in economic growth of between 4 and 6%. In this context, states had to find that balance between measures to protect the health of citizens and those to ensure the proper functioning of the economy.

Next, the paper analyzes how the COVID-19 pandemic affected the population (number of infections) and the economy (GDP growth rate) in a number of 50 countries, including all the member states of the European Union, the US, the UK and other economic powers of the world, but also some less developed countries. Is there a direct link between the partial/total lockdown measures implemented by most states on March-April 2020 and the decrease in positive disease rates and the decline of the national economy?

State (population)	**1st Quarter 2020**	**2nd Quarter 2020**	**3rd Quarter 2020**	**State (population)**	**1st Quarter 2020**	**2nd Quarter 2020**	**3rd Quarter 2020**
	*COVID-19 cases/1 mil. population** *GDP growth rate (%)*				*COVID-19 cases/1 mil. population** *GDP growth rate (%)*		
Argentina (45,356,879)	23.2 -4.2	1,399.5 -16.2	15,134.9 -	*Italy* (60,426,920)	1,750.5 -5.5	2,231.2 -13.0	1,229.0 16.1
Australia (25,614,523)	185.9 -0.3	120.0 -7.0	751.2 -	*Japan* (126,324,219)	17.2 -0.6	129.9 -8.2	509.9 5.0
Austria (9,026,432)	1,127.8 -2.5	840.4 -12.1	2,996.4 11.1	*Latvia* (1,877,938)	211.9 -2.3	309.4 -7.1	375.9 6.6
Belgium (11,609,313)	1,100.4 -3.4	4,190.8 -11.8	4,796.8 10.7	*Lithuania* (2,707,204)	198.4 0.0	472.8 -5.9	1,062.4 3.7
Brazil (213,147,624)	26.8 -2.5	6,581.2 -9.7	15,975.3 -	*Luxembourg* (629,904)	2,829.0 -1.4	2,752.8 -7.2	7,926.6 -
Bulgaria (6,927,792)	57.6 0.4	662.5 -10.1	2,287.0 4.3	*Malta* (442,003)	382.4 -2.6	1,133.5 -11.6	5,402.7 -
Canada (37,870,757)	227.4 -2.1	2,524.2 -11.5	1,440.5 10.0	*Mexico* (129,458,236)	8.7 -1.2	1,751.0 -17.1	4,127.1 12.0
Czech Republic (10,716,756)	309.2 -3.3	808.7 -8.7	5,485.9 6.2	*Netherlands* (17,149,704)	734.4 -1.5	2,197.0 -8.5	4,115.1 7.7
Chile (19,179,984)	167.1 3.0	14,402.6 -13.2	9,573.4 -	*New Zealand* (5,002,100)	129.3 -1.4	176.1 -12.2	61.6 -
China (1,439,323,776)	56.7 -10.0	1.4 11.7	1.3 2.7	*Norway* (5,437,731)	853.5 -1.5	779.4 -4.7	946.7 4.6
Colombia (51,093,242)	17.7 -2.1	1,897.3 -14.9	14,323.5 -	*Poland* (37,830,343)	61.1 -0.3	848.0 -9.0	1,510.0 7.7

[15] ***, *Evaluating the Initial Impact of COVID Containment Measures on Activity*, OECD Policy Responses to Coronavirus (COVID-19), 27 March 2020, pp. 1-2.

State (population)	1st Quarter 2020	2nd Quarter 2020	3rd Quarter 2020	State (population)	1st Quarter 2020	2nd Quarter 2020	3rd Quarter 2020
	*COVID-19 cases/1 mil. population** *GDP growth rate (%)*				*COVID-19 cases/1 mil. population** *GDP growth rate (%)*		
Croatia (4,095,283)	211.7 -1.3	466.4 -15.0	3,373.6 -	*Portugal* (10,185,020)	831.6 -4.0	3,649.2 -13.9	3,296.0 13.2
Cyprus (1,210,780)	216.4 -0.9	607.9 -13.1	625.2 9.4	*Romania* (19,187,059)	117.0 0.0	1,288.6 -12.2	5,243.2 5.6
Denmark (5,800,171)	493.1 -1.6	1,708.2 -6.8	2,625.8 4.9	*Russia* (145,958,985)	16.0 -0.9	4,422.6 -3.2	3,620.4 -
Estonia (1,326,885)	561.5 -2.2	937.5 -5.6	1.040.0 -	*Saudi Arabia* (35,023,049)	44.6 -0.9	540.4 -4.9	4,105.4 -
Finland (5,544,089)	255.8 -1.4	1,045.4 -4.4	501.1 2.6	*Slovakia* (5,460,678)	66.5 -5.1	238.8 -8.3	1,551.8 11.7
France (65,330,016)	797.9 -5.9	1,724.7 -13.7	6,106.4 18.2	*Slovenia* (2,079,050)	385.8 -4.7	383.8 -9.9	1,967.2 -
Germany (83,888,647)	856.0 -1.9	1,427.4 -9.8	1,157.2 8.2	*South Africa* (59,598,116)	22.7 -0.5	2,514.4 -16.4	8,777.6 -
Greece (10,403,001)	126.3 -0.7	201.4 -14.0	1,448.2 -	*South Korea* (51,286,469)	190.8 -1.3	58.8 -3.2	214.7 1.9
Hungary (9,650,711)	51.0 -0.4	379.6 -14.6	2,311.3 11.3	*Spain* (46,761,875)	3,603.8 -5.2	1,927.6 -17.8	12,028.3 16.7
Iceland (342,106)	3,317.7 -5.7	2,014.0 -9.1	2,642.5 -	*Sweden* (10,123,802)	477.6 0.2	6,225.8 -8.3	2,565.3 4.3
India (1,385,271,269)	1.0 0.7	421.9 -25.2	4,132.4 -	*Switzerland* (8,679,256)	1,913.2 -1.9	1,740.8 -7.3	2,485.0 -
Indonesia (274,645,527)	5.6 -0.7	199.7 -6.9	839.7 3.1	*Turkey* (84,691,021)	159.8 -0.1	2,200.6 -11.0	1,402.2 -
Ireland (4,959,167)	652.3 -2.1	4,482.8 -6.1	2,155.4 -	*United Kingdom* (68,025,098)	335.1 -2.5	3,828.9 -19.8	2,673.6 15.5
Israel (9,197,590)	582.5 -1.8	2,162.1 -8.5	23,946.5 8.4	*United States* (331,759,224)	596.1 -1,3	7,674.4 -9.0	14,319.3 7.4

Figure no. 2: Dynamics of the number of COVID-19 cases reported per 1 million population[16] and the quarterly GDP growth rate[17], compared to the previous quarter[18]

[16] Data processed from ***, *COVID-19 Coronavirus Pandemic*, Worldometer, 2020, URL: https://www.worldometers.info/coronavirus, accessed on 06.10.2020.

As we can see in the table above, containment measures to prevent and combat the spread of coronavirus (partial/total lockdown in March-April) led to an economic decline in the second quarter of 2020 in all analyzed countries. The exception is, of course, China, which experienced the effects of the pandemic on economic activity a few months earlier than other states, registering a negative growth rate (-10%[19]) in the first quarter. The economic decline was extremely strong in India and the UK, with decreases of 20-25% in the second quarter from the previous quarter, followed by Spain, Mexico, South Africa, Argentina, Croatia and Colombia, where GDP's growth rates were almost and even over 15% lower. In other countries, the impact of the pandemic on economic activity was less severe, with Russia, South Korea, Finland, Norway and Saudi Arabia experiencing declines in economic growth in the second quarter by up to 5 percentage points.

Already at the end of the first quarter of 2020, China, along with the largest Western economies – the US, Spain, Italy, Germany, France – had been hit hard by the first wave of the pandemic, with a total number of COVID-19 cases of over 50,000[20]. Other Western European countries have also seen increases in the rate of infection with the new coronavirus by more than 10,000 cases, such as the UK, Switzerland, Belgium, the Netherlands, Austria, but also Turkey. The second quarter came with a record number of new positive cases in almost all analyzed countries, with the exception of Australia, Austria, Iceland, Norway, South Korea and Switzerland, which have succeeded through the measures taken to temporarily stop the spreading of the virus. In this quarter, almost all states felt the effects of containment measures on the economy.

If we report the number of new COVID-19 cases in the second quarter of 2020 to 1 million inhabitants, we notice that, on the one hand, countries that have not taken harsh containment measures have registered an increased infection rate to over 5,000 cases: Chile – 14,403, the US – 7,674, Brazil – 6,581, and Sweden – 6,226. They are closely followed by a number of EU member states, where the measures taken have been less drastic, such as Ireland, Belgium, the UK, Portugal, but also Russia. On the other hand, an extremely small proportion of new positive cases were recorded in Asian countries – China, South Korea, Japan, Indonesia – as well as Australia and New Zealand. Of course, there are also a number of European countries that have managed to reduce this rate in the second quarter compared to the first quarter of 2020, such as: Austria, Luxembourg, Norway, Switzerland, Slovenia or Spain.

We therefore ask ourselves whether the states that have faced the strongest economic decline have managed, as we would expect, to protect the health of their population? Contrary to the idea that there is a certain balance, we notice that the countries that have suffered the most severe economic downturn – such as Spain and the UK – are generally among those with the highest rates of new coronavirus infection. The reverse is also true: countries where the economic impact has been modest – such as South Korea, Ireland and Lithuania – have succeeded to keep the number of new COVID-19 cases low. Of course, this balance depends on a multitude of factors, such as: the extent of the containment measures taken, the structure

[17] ***, *GDP and employment flash estimated for the third quarter of 2020*, News Release 168/2020, Eurostat, 13 November 2020, p. 3; ***, *Quarterly Growth Rates of real GDP, change over same quarter, previous year*, OECD.Stat, URL: https://stats.oecd.org/index.aspx?queryid=350, accessed on 06.10.2020.

[18] Note: * This indicator has been estimated as a ratio between the total number of COVID-19 new cases registered in that quarter x 1 million inhabitants / total population of the respective country

[19] ***, *Quarterly Growth Rates of real GDP, change over same quarter, previous year*, OECD.Stat, URL: https://stats.oecd.org/index.aspx?queryid=350, accessed on 09.10.2020

[20] ***, *WHO Coronavirus Disease (COVID-19) Dashboard*, World Health Organization, 2020, URL: https://covid19.who.int, accessed on 14.10.2020.

of the economy, the health of the population, etc. For example, Greece, a country where tourism is a key element of its economy, recorded an GDP dropping of 14%, as the rate of new COVID-19 cases increased very little from 126 in the first quarter to 201 in the next quarter.

Sweden, which did not take harsh containment measures[21], managed to keep the economic decline below 10%, but the number of new infections exploded from 478 cases/1 million inhabitants in the first quarter to 6,226 cases/1 million inhabitants in the second quarter. Taking the case of this Scandinavian country and comparing it with countries that have taken complete lockdown measures, such as Spain, Italy or France[22], it is obvious that the last three countries have managed to maintain the positive rate at 1,700 cases per 1 million inhabitants in the second quarter, almost 4 times less than Sweden. On the contrary, comparing the economic performance, it can be seen that the GDP of Europe's three economic powers have contracted by more than 13% between April and July 2020, almost double that of the Swedish economy. Also, countries with similar economic decline registered very different infection rates. If we compare the US and Sweden with the Czech Republic and Poland, we notice that all four countries faced economic contractions of about 8-9% in the second quarter of 2020, but new COVID-19 cases vary significantly: the US and Sweden have 7 to 10 times more cases per 1 million inhabitants. If we compare the US and Sweden with Japan, then the ratio is more unbalanced – almost 60 times more cases in the first two.

In conclusion, we cannot say with certainty that there is a clear link between protecting people's health and protecting the economy, in the sense that keeping the spread of COVID-19 pandemic under control meant a severe economic decline or reverse. Rather, the relationship we see between the impact of the pandemic on health, on one hand, and economy, on other, goes in the opposite direction – government that effectively controlled the pandemic outbreak may have adopted the best economic strategy.

Conclusions

The COVID-19 pandemic and the associated health crisis have created a major dilemma for national authorities: strict containment measures to prevent and combat the spread of coronavirus with benefic effects for the population's health or less harsh restrictions on people movement and economic and social activities with positive effects for the national economy. It is true that the partial or complete lockdown imposed by most states in March-April 2020 have led to retaining in acceptable limits or even to reducing the number of cases, but economic growth slowed considerably in the second quarter in all developed or underdeveloped countries. The easing of the restrictions, starting with May, relaunched the economic activity, but the number of new COVID-19 cases and deaths reached alarming levels. Although experts say that some states relaxed the restrictions too soon, probably sooner or later, they would have reached the same situation.

However, the above analysis shows that there is no easy solution or a specific balance between protecting the health of the population and the smooth running of the economy. Some countries have taken containment measures that have led to a reduction in the number of infections, but they have affected the economy. Others have managed to protect to some

[21] Alice Baudry, "Covid-19: Still No Sign of Lockdown for Sweden", *Institut Montaigne*, 3 April 2020, URL: https://www.institutmontaigne.org/en/blog/covid-19-still-no-sign-lockdown-sweden, accessed on 14.10.2020.
[22] ***, "Coronavirus: What are the lockdown measures across Europe?, *Deutsche Welle*, 14 April 2020, URL: https://www.dw.com/en/coronavirus-what-are-the-lockdown-measures-across-europe/a-52905137, accessed on 16.10.2020.

extent both the population and the economy, and in other cases the measures taken or not have led to an increase in the number of COVID-19 diseases and economic decline. The second wave of the pandemic, triggered in early autumn, is much more aggressive, with many states already facing record levels of new infections. It is likely that, based on the lessons learned in the first stage of the pandemic, the authorities will be able to find the balance in the application of measures to prevent and combat the pandemic in order to protect the health and the well-being of citizens and the national economy.

Undoubtedly, the COVID-19 pandemic will be stopped with the support of a vaccine – which will become a certainty at the beginning of next year –, but its effects on society and the economy will continue to manifest themselves for some years to come. There is still a need for solidarity and cooperation in implementing and complying with all measures, procedures, plans and strategies that increase the resilience and response capacity of nation states and the international community to such health crises.

BIBLIOGRAPHY:

1. ***, "Coronavirus: What are the lockdown measures across Europe?, *Deutsche Welle*, 14 April 2020, URL: https://www.dw.com/en/coronavirus-what-are-the-lockdown-measures-across-europe/a-52905137
2. ***, "Primul caz de coronavirus în România", *Digi24*, 26 February 2020, URL: https://www.digi24.ro/stiri/actualitate/primul-caz-de-coronavirus-in-romania-1266806.
3. ***, *COVID-19 Coronavirus Pandemic*, Worldometer, 2020, URL: https://www.worldometers.info/coronavirus
4. ***, *Evaluating the Initial Impact of COVID Containment Measures on Activity*, OECD Policy Responses to Coronavirus (COVID-19), 27 March 2020.
5. ***, *GDP and employment flash estimated for the third quarter of 2020*, News Release 168/2020, Eurostat, 13 November 2020.
6. ***, *Global Economic Prospects*, A World Bank Group Flagship Report, Washington, DC, June 2020.
7. ***, *Past pandemics*, World Health Organization, URL: https://www.euro.who.int/en/ health-topics/communicable-diseases/influenza/pandemic-influenza/past-pandemics.
8. ***, *Quarterly Growth Rates of real GDP, change over same quarter, previous year*, OECD.Stat, URL: https://stats.oecd.org/index.aspx?queryid=350
9. ***, *WHO Coronavirus Disease (COVID-19) Dashboard*, World Health Organization, 2020, URL: https://covid19.who.int
10. ***, *WHO Director-General's opening remarks at the media briefing on COVID-19*, WHO, 11 March 2020, URL: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020
11. ***, *World Economic Outlook Update: A Crisis Like No Other, An Uncertain Recovery*, International Monetary Fund, Washington, DC, June 2020.
12. ***, *World Economic Outlook: A Long and Difficult Ascent*, International Monetary Fund, Washington, DC, October 2020.
13. ***, *World Economic Outlook: The Great Lockdown*, International Monetary Fund, Washington, DC, April 2020.
14. ***, *World Economic Situation and Prospects as of mid-2020*, Department of Economic and Social Affairs, United Nations, New York, 2020.
15. BĂHNĂREANU, Cristian, "The Economic Impact of COVID-19 Pandemic at the Beginning of 2020", *Strategic Impact*, No. 2/2020, Centre for Defence and Security Strategic Studies, "Carol I" National Defence University Publishing House, Bucharest, 2020.
16. BAUDRY, Alice, "Covid-19: Still No Sign of Lockdown for Sweden", *Institut Montaigne*, 3 April 2020, URL: https://www.institutmontaigne.org/en/blog/covid-19-still-no-sign-lockdown-sweden

17. CÁRDENAS, Mauricio, "Looking at the Bright Side: 10 Positive Effects of the Pandemic", *Americas Quarterly*, 13 July 2020, URL: https://www.americasquarterly.org/article/looking-at-the-bright-side-10-positive-effects-of-the-pandemic
18. FIFIELD, Anna, "China's economy bounces back more quickly than expected from coronavirus", *The Washington Post*, 16 July 2020, URL: https://www.washingtonpost.com/world/asia_pacific/chinas-economy-bounces-back-more-quickly-than-expected-from-coronavirus/2020/07/16/b4285da2-c67a-11ea-a825-8722004e4150_story.html
19. KOSE, Ayhan; Naotaka SUGAWARA, "Understanding the depth of the 2020 global recession in 5 charts", *World Bank Blogs*, 15 June 2020, URL: https://blogs.worldbank.org/opendata/understanding-depth-2020-global-recession-5-charts
20. McKIBBIN, Warwick; Roshen FERNANDO, *Global macroeconomic scenarios of the COVID-19 pandemic*, CAMA Working Paper 62/2020, Australian National University, June 2020.
21. SANDFORD, Alasdair, „Coronavirus: Half of humanity now on lockdown as 90 countries call for confinement", *Euronews*, 3 April 2020, URL: https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou

STRATEGIC CULTURE AND SECURITY CULTURE – A COMPARATIVE ANALYSIS – THE RELEVANCE OF SECURITY CULTURE IN THE 21ST CENTURY

Antonia Teodora MARIȘ
Lieutenant, Ph.D. Student within "Carol I" National Defence University,
Bucharest, Romania. E-mail: antonia.maris@yahoo.com

Abstract*: The present material proposes, in its first chapter, a conceptual delimitation for the terms strategic culture and security culture, starting with security. Further on in the paper, we will make a comparative analysis between the two, at the same time dwelling on the shift from strategic culture to security culture and arguing the relevance of the latter, in the context of the current century, making specific remarks to Romania. The 21st century outlines new challenges in developing and consolidating security culture by introducing a myriad of factors that need to be taken into consideration. Spectacular changes in technological progress, the ubiquity of digital technologies, the digital revolution, the global digital order, the increasing importance of digital platforms, the speed with which information is transmitted, algorithmisation of personal life, the power to change and direct public opinion, cultivation and aggravation of disputes are only a few of the characteristics of the 21st century.*

Keywords: *security culture; strategic culture; security threats; national security; raising awareness; public opinion.*

Introduction

The present material proposes a conceptual delimitation for the following terms: *security, strategic culture, security culture*. Also, this paper highlights the role of security culture as an essential element for the security and well-being of a state actor, as well as how the realities of the present century outline new security challenges.

All these specific advances of the current century also generate new risks, threats and vulnerabilities: the fake news phenomenon, misinformation, the desire to change the level of population trust indices in the governing structures, the digital revolution, the dominant technologies that manage to change knowledge monopolies, the growing importance of digital platforms. By making use of these factors, an adversary can destabilize an entire society, slowly moving towards delegitimizing a government. Influence activities directed at the populations aim to disrupt and create distrust. The "divide and rule" approach is to create as many cleavages on as many levels as possible. An adversary, as a large power, would then more easily deal with a multi-fragmented society. All actions that determine/participate/help mitigate these new vulnerabilities, threats and risks are part of security culture. Using these new challenges as a starting point, a first step is increasing awareness among the population regarding their existence. Two of the most important steps in establishing security fundamentals of a state are identifying its vulnerabilities and building a strong security culture.

1. Conceptual delimitations

Over time, there has been a search for a way to define security in a comprehensive manner that contains all the aspects it touches. Definitions of this concept from different angles will be presented in the following lines.

In his paper entitled *Peoples, States and Fear: an agenda for international security studies in the post-cold war era,* Barry Buzan presented several different approaches in trying to define security[1]:

• "Security, in an objective sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked"[2];

• "Security itself is a relative freedom from war, coupled with a relatively high expectation that defeat will not be a consequence of any war that should occur"[3];

• "The ability of a nation to pursue successfully its national interests, as it sees them, any place in the world"[4];

• "Preservation of way of life acceptable to the …people and compatible with the needs and legitimate aspirations of others"[5];

• "Assurance of future well-being"[6];

• "The ability to withstand aggression from abroad"[7];

• "A nation is secure to the extent to which it is not in danger of having to sacrifice core values if it wishes to avoid war, and is able, if challenged, to maintain them by victory in such a war"[8].

Security is also a fundamental right of any human being. It represents a state in which dangers and conditions that could create physical, psychological or material harm are controlled in a manner that allows the defence of health and welfare of individuals and communities.[9].

Security is a basic need of any human being, so it is also a permanent concern of the community. Moreover, in the hierarchy of needs found in Abraham Maslow's[10] pyramid, the need for safety and security appears immediately after the primary needs. It can be considered that individual security results from the dynamic balance that is established between the different components of the environment (cultural, technological, social, political, etc.).

In my opinion, security is responsible for countering threats and maintaining a state of peace by defending values, identity and integrity of a state or nation.

---

[1] Barry Buzan, *People, states & fear: an agenda for international security studies in the post-cold war era*, Published by ECPR Press, 2007, p. 36.
[2] Arnold Wolfers, *Discord and collaboration*, apud Barry Buzan, *op. cit.*, p. 36.
[3] Ian Bellany, *Towards a theory of international security*, apud Barry Buzan, *op. cit.*, p. 36.
[4] Penelope Hartland-Thunberg, *National Economic Security: inter dependence and vulnerability*, apud Barry Buzan, *op. cit*., p. 36.
[5] National Defense College, Canada, *Course document*, apud Barry Buzan, *op. cit*., p. 36.
[6] Laurence Martin, *Can there be national security in an insecure age*, apud Barry Buzan, *op. cit*., p. 36.
[7] Giacomo Luciani, *The economic content of security*, apud Barry Buzan, *op. cit*., p. 36.
[8] Walter Lippmann, *US foreign policy: shield of the Republic*, apud Barry Buzan, *op. cit*., p. 36.
[9] Neculai Stoina, "Securitatea umană și cultura de securitate", in *Sesiunea anuală de comunicări științifice cu participare internațională STRATEGII XXI/2006*, intitulată Securitatea și apărarea spațiului sud-est european, în contextul transformărilor de la începutul mileniului III, Secțiunea 3, Apărare și securitate națională, Constantin Moștoflei (coordinator), CDSSS, "Carol I" National Defence University Publishing House, Bucharest, 2006, pp. 582-594.
[10] *Psihologia motivațională a lui Abraham Maslow*, Scientia.Ro, URL: https://www.scientia.ro/homo-humanus/introducere-in-psihologie-russell-a-dewey/7094-psihologia-motivationala-a-lui-abraham-maslow.html, accessed on 07.02.2019.

According to Barry Buzan's theory, security has five dimensions in interaction and complementarity with each other, each regulating different aspects of social life:

• military (military security concerns the two-level game of offensive and defensive capabilities of states);

• politics (political security concerns the organizational stability of states, governance systems and ideologies that give them legitimacy);

• economic (economic security concerns access to the resources, markets and capital needed to support acceptable levels of welfare and power of the state);

• societal (the social security concerns the sustainability, under acceptable evolutionary conditions, of the traditional patterns of the language, culture and religion, as well as of the national customs and identity);

• environmental (environmental security concerns the maintenance of the local and global biosphere as an essential support on which all other human activities depend)[11].

Over the last few decades, the definition of security has been expanded to manage with the 21st century globalized worldwide community, its fast improvements and worldwide dangers that have risen from this continuous evolution. One such comprehensive definition has been submitted by Nayef Al-Rodhan. His proposed "multi-sum security principle" is based on the assumption that "in a globalized world, security can no longer be thought of as a zero-sum game involving states alone. Global security, instead, has five dimensions that include human, environmental, national, transnational, and transcultural security, and therefore, global security and the security of any state or culture cannot be achieved without good governance at all levels that guarantees security through justice for all individuals, states, and cultures"[12].

Insuring security is a common interest of the states, and this can be better done of a coordinated manner. This idea is highlighted in the European Union's Global Strategy: "none of our countries has the strength nor the resources to address these threats […] of our time alone"[13].

In order to talk about security at a general level, one must start from the idea of national security. At the base of national security, there are two vectors: national values and national interest[14]. National values are elements of a spiritual, cultural and material nature that define the identity of a nation. Referring to Romania, by protecting, promoting and defending national values, the essential conditions of the existence and dignity of the citizens and the Romanian state are ensured, in accordance with the provisions of the Constitution[15]. The second dimension, the national interest, is in fact the objectives of the state concerned.

In order to define *security culture*, we are also interested in delimiting the concept of *culture* and the influence of culture on human perceptions and behaviour and especially their manifestation.

Thus, *culture* can be understood as a collection of common rules, traditions, customs, attitudes, values, rules and practices specific to a particular group. Michael Albert stated the following: if we want to designate with a single word a set of individual behaviours shared by

[11] Barry Buzan, *op. cit.*, pp. 19-20.
[12] Nayef Al-Rodhan, *The Five Dimensions of Global Security: Proposal for a Multi-sum Security Principle*, Berlin, 2007, pp. 15-16.
[13] *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign and Security Policy*, URL: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, p. 3.
[14] Ion Zamfirache, *Despre securitate în contextul globalizării*, Editura Didactică și Pedagogică, Bucharest, 2014, p. 13.
[15] Nicu Sava, *Teoria și practica securității, suport de curs*, Bucharest, 2007, p. 38.

the majority of a population, the assembly that relies on institutions, on rules recognized by everyone and on a common heritage, we are obliged to talk about culture[16].

Geert Hofstede defines culture as mental software, a collective programming of the mind, defining for each social group[17]. This gives specificity and originality to each group, but can also be a source of conflict.

Security culture represents a sum of values, norms, attitudes and actions that determine the understanding and assimilation of the concept of security and of the other derived concepts: national security, international security, collective security, insecurity, security policy, etc.[18].

Security culture can also be defined as the sum of beliefs, values and practices of institutions and individuals that determine what is considered to be a danger or insecurity in the broadest sense and which are the methods, means, and ways of counteracting them[19].

Nicole Gnesotto defined security culture as "the purpose and means of generating a common thought, compatible reactions, and coherent analysis – that is, an increasingly European strategic culture which transcends national security interests and cultures" [20].

The term "security culture" was used mainly after the collapse of communism, precisely because it was a defining part of the new security climate. This concept requires a permanent adaptation to the specific of the present.

In order to promote and root security culture at the individual level, it is very important to customize it to the specific values and principles of the respective nation. A viable security environment is based on respecting the specificity and vision of the population, ideals, standards, conceptions, opinions, traditions, etc.[21].

It is almost impossible to accurately measure security culture, but assessments can be made by evaluating the following indicators[22]:

• the individual initiative: the degree of involvement and taking responsibility;

•tolerance acquired through risk exposure: the degree of risk taking, of being offensive through innovation;

• direction: the extent to which the objectives, interests and tasks set are clear, conclusive, efficient;

• integration: how the structures implement the principle of effort coordination;

• control: the degree to which certain rules and regulations are applied with direct supervision of employees;

• identity: the extent to which employees identify themselves with the organizational structure, the way they perceive and treat the organizational objectives as their own performance objectives;

• reward system: the degree to which these are based on employee performance;

• conflict tolerance: the degree to which employees are encouraged to resolve conflicts;

• communication procedures: achieving efficient communication on different levels.

---

[16] Michael Albert, *Capitalism contra capitalism*, Editura Humanitas, Bucharest, 1994, p. 99.

[17] Geert Hofstede, Gert Jan Hofstede, Michael Minkov, *Culturi și organizații. Softul mintal*, trad. Mihaela Zografi, Published by Humanitas, 2012, p. 34.

[18] Neculai Stoina, *op. cit.*, p. 583 (author's translation).

[19] Christopher Daase, *National, societal and human security: On the transformation of political language*, Historical Social Research, 2010, p. 22.

[20] Nicole Gnesotto, *For a Common European Security Culture*, in WEU-ISS Newsletter 31, October, 2000.

[21] Sorin Topor, Mihai-Stefan Dinu, *Culture and e-learning-global challenges and perspectives*, The International Scientific Conference eLearning and Software for Education, Vol 1, "Carol I" National Defence University, Bucharest, 2014.

[22] Neculai Stoina, *op. cit.*, p. 585.

Security culture, among its many facets, also has an educational side. Each organisation should benefit from a security education (lessons learned, standards for applying certain measures, how to analyse media publications, etc.). Cultural influences, economics or geography are just a few of the factors that can decide the form of a state-specific security culture. According to C. Gray, "security culture refers to those mental archetypes, traditions and socially transmitted preferred modes of action which are more or less specific to a security community located in a certain geographical area"[23]. Additionally, according to A. Latham, security culture encompasses "a set of resounding ideas, crystallised following a long historical experience and deeply rooted in common conscience or common judgement"[24].

Until recent times, security was based mainly on hard security dimensions (military), while the soft dimensions (non-military, like cultural influences, economics, geography) were considered in a limited capacity. On this contemporary level of international relations, the balance has changed, shifting the roles of both soft and hard dimensions, in such a way that "soft power" is now taking the lead. In addition to soft power, smart power (the combination of soft and smart power) plays a significant role in contemporary International Relations.

This is taking place on the national level, as well as beyond borders, on the international scale. Economic and/or political instability are two factors slowing this adaptation.

The economical and geographical dimensions are widely accepted at NATO level as being highly influential when it comes to security.

The risks and threats to security have evolved with time; their forms of manifestation are increasingly difficult to detect and counter. Defence must be carried out both individually (by each state, through an internal policy, individual strategies) and through collective forms of defence, adapted to the characteristics of the current security environment. Both forms of security ensure the establishment and maintenance of a stable security climate nationally and internationally[25].

Creating and promoting a culture of security among the members of society is a priority on the agenda of state leaders. Informing the population about the relevant aspects of this field and the permanent consolidation of this type of culture is the foundation of a strong security culture.

2. Going from strategic culture to security culture

The transition from *strategic culture* to *security culture* was made, rising to the highest level the subjects previously considered to be of secondary importance. An obvious distinction between the two concepts is the attention given by the strategic culture to the military component. Security culture does not replace strategic culture, but complements it with a number of topical areas and approaches. The actors did not give up the force policy; we are witnessing an adaptation, a new approach that limits the use of force and achieves goals through other methods.

There is a high degree of overlap between the two terms: what some authors define as strategic culture, others see as security culture. Jolyon Howorh bases this situation on the fact

[23] Colin S. Gray, *War, Peace and Victory (Strategy and Statecraft for the Next Century),* apud. Ciprian Lungu, Ruxandra Buluc, Ioan Deac, *Raport. Promovarea culturii de securitate*, București, 2018, p. 3.

[24] Andrew Latham, *Constructing National Security (Culture and Identity in Indian Arms Control and Disarmament Practice)*, in *Contemporary Security Policy* 19, apud Lungu, Buluc, Deac, *op. cit*, p. 4.

[25] Sorin Topor, "Informații despre amenințări și menținerea controlului într-un mediu conflictual modern", in *Buletinul Universităţii Naţionale de Apărare Carol I*, nr. 3/ 2018, "Carol I" National Defence University Publishing House, Bucharest, 2018.

that the phrase "strategic culture" sounds more heroic, compared to the phrase "security culture", which has a rather neutral resonance[26].

Another reason why the confusion between the two synthases exists is that security culture field originates from the first studies that addressed strategic culture. The first association between the terms *strategy* and *culture* was made by the American academic Jack Snyder in a study from the 1970s on USSR and US approaches in the field of nuclear strategy.

Strategic culture actually describes the collective mindset of a society or nation; thus described, the phrase can be easily categorized into the security culture category. Canadian researcher Keith R. Krause is one of the researchers interested in the subtle differences between these two concepts. As a result of its in-depth analysis, he has drawn up an explicit diagram with the differences (relative differences, with many aspects in common) between strategic culture and security culture, as can be seen in **Table no. 1**.

Table no. 1: Strategic culture and security culture[27]

Strategic culture	Security culture
- The experience of war and peace - The role of the armed forces - Various ways of perceiving threats - Security doctrines - Images of the enemy - The unilateral or mutual security model	- Beliefs - Traditions - Attitudes - Rooted symbols that are widely spread all of which influence the way a state's or society's interests and values regarding security are perceived, expressed and tracked.

Strategic culture analyses and focuses more on power and war issues, while security culture relies on traditions, attitudes, values, mental training to support the process of stability, peace and security. In the society we live in, values and culture play a very important role in the field of security.

A very important aspect for the field of security studies is that differences between cultures can lead to strong conflicts when they meet. These cultural nuances are relevant and necessary within the framework of security strategies, the specificity of the peoples and nations referred to is the foundation of the future directions. The conflicts in Afghanistan, Kosovo, the Central African Republic, Syria – are examples of conflicts in which the cultural aspect (i.e. cultural differences) plays an important role.

The transformations through which the Western world went through the 1990s were profound and emphasized the need to study in depth the phenomenon of security culture with all that it implies (values, traditions, culture, human rights, collective attitude, national interests, etc.).

Security culture, unlike strategic culture, also refers to the way of thinking, acting and reacting on a collective level; it is based on the values, principles and culture of a nation. Strategic culture has a narrower meaning, an analysis and a combination of lessons learned, thus, being a part of security culture.

John C. Garnett, in an article published in 1996, argues that security is an important value in itself[28]. The attitude and level of understanding of the collective or of the nation regarding certain values and what represents the security of the nation, as well as how the

[26] Jolyon Howorth, *Security and Defence in the European Union*, Published by Palgrave Macmillan, 2007, p. 178.
[27] *Ibidem*, p. 201.
[28] John C. Garnett, *European Security after the Cold War*, in M.J., DAVIS (ed.), *Security issues in the Post-Cold War World*, Edward Elgar, Cheltenham, UK, 1996, pp. 12-38.

population is prepared to respond to certain threats against them, represents in fact the security culture. Understanding the different ways of perceiving security needs, the need for common security constitutes another step in achieving a security culture.

There are national characteristics, or at least a common form of manifestation and feeling, specific to each state. Even if they are geographically close, they may have totally different perspectives on the world and life. This specificity of each state can also represent a cultural conditioning that needs to be taken into account in creating strategic culture. Given these particularities, these cultural differences, security culture cannot be the same in Japan and France. Respecting cultural stereotypes is actually the foundation of a strong security culture.

Starting from one of the realities of the current century, the fake news phenomenon, we analysed a report made in order to determine, among others, to what extent a mature security culture can lead to the judicious identification of what is fake news[29]. One of the questions in the report aimed to prioritize four possible objectives of promoting the security culture that contribute to identifying fake news and limiting the effects of digital misinformation. Participants in the study appreciate that promoting security culture has an active role in identifying and counteracting the effects of fake news, especially by ensuring a minimum knowledge for a wider audience on the concept of security (74.4%) and developing the citizens' ability to understand security risks, challenges and threats (71.7%). A less important role would be to adapt the behaviour of individuals, groups and society as a whole to specific security conditions (34.5%) and the application by citizens of norms, rules, standard procedures for action in the field of security (27.3%)[30].

The new types of threats, the increasing importance of the alliances in the consolidation of national interests were the basis for the need to pay a deep attention to the formation and development of a security culture adapted to the cultural characteristics specific to each state. In order for a country to maintain its sovereignty and fulfil its goals and interests, it must form its own security culture, including when alliance strategy becomes dominant[31]. Romania took notice of all these changing dynamics and made it a point to update its strategies with the understanding of the importance and relevance of this centre of gravity.

According to point 51 of the Romanian National Defence Strategy for 2020-2024, "a precarious security culture constitutes a societal vulnerability (…)"[32]. The same document also states, under sub-chapter 4.3. – *Vulnerabilities*, point 168, that "a low security culture among the civilian society and at the level of the decision making apparatus can be exploited by hostile informational entities with the purpose of gathering information or conducting influence operations". Having identified these weak points, one of the lines of effort formulated with the purpose of mitigation is "developing a security culture, also through continuous education, that will promote values, norms, attitudes and actions with the purpose of enabling assimilating the concept of national security" [33].

Identifying the need to consolidate security culture as an objective in relevant strategic documents constitutes a first step in adapting national strategies to new threats that loom over the Romanian society.

---

[29] Ruxandra Buluc, Ioan Deac, Răzvan Grigoraş, Ciprian Lungu, *Cultura de securitate şi fenomenul fake news: raport*, Editura Top Form Bucureşti, 2019, p. 27.
[30] *Ibidem*, p. 136.
[31] Gheorghe Văduva, *Is there still a Romanian military thinking?*, Theory and military science magazine edited by the General Defense Staff of the Romanian Military, *Gândirea militară românească*, Published by General Defence Staff of the Romanian Military, no. 1, Bucharest, 2005, p. 112.
[32] National Defence Strategy for 2020-2024 – "Together for a secure and a prosper Romania in a world branded by new challenges", p. 12 (author's translation).
[33] *Ibidem*, p. 21.

Conclusions

While in the case of strategic culture, the focus is on the military domain, security culture comes to complement it by including several analysis sectors; security culture responds to the risks, threats and vulnerabilities specific to the 21st century, a century in which the security and importance of the individual are key concepts for ensuring the well-being of the population.

An important aspect is the degree to which population assumes behaviours in line with the concept of security culture. Popular security culture focuses on the general perceptions of who our enemies are, how they threaten us and how we can effectively defend ourselves, as well as mitigating or fully eliminating the factors that lead to vulnerabilities. In order for the population to develop a viable security culture, it must be understandable to all and widely accessible. When developing a security culture, the psycho-social level must be taken into account, which includes the values, perceptions and attitudes of the population; it is influenced and influences how different policies are applied. Security culture must take into account the new types of threats: the fake news phenomenon, the desire to create alternative realities, misinformation, dominant technologies that manage to change knowledge monopolies, the increasing importance of digital platforms through which different internal disputes are cultivated, the deepening distrust of the population in regards to political figures etc.

The technological revolution human kind was exposed to in the last few decades has generated whole new sets of unpredictable threats, risks and vulnerabilities, making it necessary to evolve from strategic culture and develop a security culture tailored to the specific of each state and a highly volatile security environment. This emerging requirement has outlined the new directions Romania is taking when it comes to addressing security concerns, defining objectives and formulating security strategies.

BIBLIOGRAPHY:

1. ***, *Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024. „Împreună, pentru o Românie sigură şi prosper într-o lume marcată de noi provocări"* (National Defence Strategy for 2020-2024. "Together for a secure and a prosper Romania in a world branded by new challenges"), URL: https://www.presidency.ro/files/userfiles/ Documente/Strategia_Nationala_ de_Aparare_a_ Tarii_2020_2024.pdf
2. ***, *European Security Strategy "A secure Europe in a Better World"*, Bruxelles, 2003.
3. ***, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, URL: https://eeas.europa.eu/archives/docs/top_stories/ pdf/eugs_ review_web.pdf
4. ***, *Psihologia motivațională a lui Abraham Maslow* (Maslow motivational psychology), URL: https://www.scientia.ro/homo-humanus/introducere-in-psihologie-russell-a-dewey/7094-psihologia-motivationala-a-lui-
5. ALBERT, M., *Capitalism contra capitalism*, Humanitas Publishing House, Bucharest, 1994.
6. AL-RODHAN, N., *The Five Dimensions of Global Security: Proposal for a Multi-sum Security Principle*, Berlin, 2007.
7. BUZAN, B., *People, States & Fear: An Agenda for International Security Studies in the Post-cold War Era*, Published by ECPR Press, 2007.
8. BULUC, R., DEAC, I., GRIGORAŞ, R., LUNGU, C., *Cultura de securitate şi fenomenul fake news: raport*, Top Form Publishing House, Bucharest, 2019.
9. DAASE, C., *National, societal and human security: on the transformation of political language*, Historical Social Research, 2010.

10. GARNETT, J., C., *European Security after the Cold War*, in M.J., DAVIS (ed.), *Security issues in the Post-Cold War World*, Edward Elgar, Cheltenham, UK, 1996.
11. GNESOTTO, N., "For a Common European Security Culture", in *WEU-ISS Newsletter 31*, October, 2000.
12. HOFSTEDE, G., HOFSTEDE, G., J., MINKOV, M., *Culturi și organizații. Softul mintal,* trad. Mihaela Zografi, Editura Humanitas, 2012.
13. HOWORTH, J., *Security and Defence in the European Union*, Palgrave Macmillan, 2007.
14. LUNGU, C., Buluc, R., Deac, I., *Raport. Promovarea culturii de securitate*, Bucharest, 2018.
15. SAVA, N., *Teoria și practica securității, suport de curs*, București, 2007.
16. STOINA, N., „Securitatea umană și cultura de securitate", in Sesiunea anuală de comunicări științifice cu participare internațională STRATEGII XXI/2006, intitulată *Securitatea și apărarea spațiului sud-est european, în contextul transformărilor de la începutul mileniului III*, Secțiunea 3, Apărare și securitate națională, Constantin MOŞTOFLEI (coordinator), CDSSS, "Carol I" National Defence University Publishing House, Bucharest, 2006.
17. TOPOR, S., DINU, M.S., "Culture and e-learning-global challenges and perspectives", *The International Scientific Conference eLearning and Software for Education*, Vol. 1, "Carol I" National Defence University, Bucharest, 2014.
18. TOPOR, S., "Informaţii despre ameninţări şi menţinerea controlului într-un mediu conflictual modern", in *Buletinul Universităţii Naţionale de Apărare Carol I*, nr. 3/ 2018, "Carol I" National Defence University Publishing House, Bucharest, 2018.
19. VĂDUVA, G., "Is there still a Romanian military thinking?", *Gândirea militară românească* (Romanian Military Thinking journal), Published by General Defence Staff of the Romanian Armed Forces, no. 1, Bucharest, 2005.
20. ZAMFIRACHE, I., *Despre securitate în contextul globalizării*, Editura Didactică și Pedagogică, Bucharest, 2014.

THE THREAT OF TERRORISM ACTING INSIDE EU BORDERS

Lara-Teodora POPESCU
Student at the Faculty of Political Science of the University of Bucharest, Romania.
E-mail: lara.popescu@yahoo.com

Abstract*: Until recently, terrorism was one of the most significant issues Europe had to face. Although terrorist acts do not represent an imminent threat to Europeans anymore, they are still a very important international problem that must be eradicated until it escalates again. This paper aims to present, through qualitative analysis, the measures and strategies taken at the European level to combat terrorism, as well as to explain why the eradication of terrorism should still be a priority for international security, despite the recognizable decrease of terrorist activity in Europe in the last few years. Towards the end of the paper, further possible actions for battling this critical threat are suggested, considering and examining the various forms that terrorism has taken over the years.*

Keywords: *terrorism; Europe; international security; threat; European Union.*

Introduction

In order to understand how terrorism has affected Europe, we need to define the act of terrorism first. From Hoffman's definition, one can understand that terrorism is, before all, a violent act or threat of violence. For an action to count as terrorism, it needs to be carried out for political, religious, or economic motives and it must be "designed to have far-reaching psychological effects beyond the immediate victim(s) or object of the terrorist attack."[1] Furthermore, terrorism must be conducted by a non-state entity or by a subnational group in order to generate power where there is none or to secure it where there is very little.[2]

Even though Europe has always been less affected by terrorism than most other regions of the world, the impact of those dreadful attacks is huge. Before the tragic 9/11 attack, nationalist groups and left-wing groups were responsible for most of the European terrorist attacks. Besides the increase of religious terrorism before, but especially after 9/11, there have been increases in terrorist incidents by Islamic terrorist groups such as Islamic State in Iraq and Syria (ISIS) or Al-Qaeda. Those attacks, conducted by Islamic extremists, have been correlated with increased activity by right-wing extremist groups.[3] Before 2014, which is considered to have been the year with most people killed worldwide because of terrorism,[4] most of the Islamic terrorist activity was associated with Al-Qaeda. The 2004 Madrid train bombings, which killed 193 civilians, was the deadliest European attack from that period. Between 2014 and 2016, there has been the highest rate of attack plots per year, with most of the activity being encouraged by the Islamic State of Iraq and the Levant (ISIL),

[1] Bruce Hoffman, *Inside Terrorism*, Columbia University Press, New York, 2006, pp. 40-41.
[2] Hoffman, *Inside Terrorism*, p. 41.
[3] David Martin Jones et al., *Handbook of Terrorism and Counter Terrorism Post 9/11*, Edward Elgar Publishing Cheltenham, UK, 2019, pp. 267-275.
[4] Erin Miller, Gary LaFree, and Laura Dugan, "Terrorism Fatalities", 2018, URL: https://www.start.umd.edu/gtd/, accessed at 05 August 2020.

also known as ISIS.[5] As for 2017, Europol registered the May 2017 Manchester Arena bombing as the deadliest attack of the year, with 22 people killed and over 500 injured.[6] In 2018, the number of attacks significantly decreased, with a total of 13 people killed and 46 injured,[7] while in 2019 ten people died as a result of terrorist attacks in the EU and 27 people presented injuries.[8]

In the last few years, there has been a noticeable decrease in the number of completed terrorist attacks due to the improved strategies and measures taken by international counter-terrorist organizations. However, studies show that from 1970 to 2018, worldwide terrorism has become more frequent and deadlier. As technology developed, a new wave of terrorism started emerging, culminating with the development of Internet terrorism. Nowadays, terrorist organizations are able to communicate, advertise, and fundraise in unimaginable ways.

Even if we cannot trace exactly the beginnings of terrorism, its most destructive period begun at the same time as the invention of dynamite and automatic weapons. Until then, "terrorist attacks" were mainly one-on-one killings.[9] Therefore, one can affirm that terrorism, as it is known nowadays, started after World War II.

The most devastating (and perhaps even the most common) tactic of terrorism is bombings. The methods in which explosives are used are various: car bombs, strapped to the bodies of individuals, etc. At this point, one can talk about another terrorism tactic - suicide terrorism, considered the most aggressive form of terrorism. Regarding the catastrophic effects of "suicide attacks", Halder emphasizes how the attack from 11 September 2001 changed the vision of the world concerning terrorism (the 9/11 attack was, at the same time, an aircraft hijacking and a suicide attack).[10]

Furthermore, as new vulnerabilities are being created by the computer dependence of every infrastructure, cyberterrorism starts to be more and more dangerous every day. As numerous reports show, cyberattacks "has meant little more than propaganda", but we should still consider the threat as imminent.[11]

1. Past measures and strategies taken at European level

Before the 9/11 terrorist attack, the EU's institutional framework did not cover cooperation in the field of counter-terrorism. This lack of strategy at the European level allowed jihadist movements to settle in the 1990s in London, the city becoming the European

[5] Petter Nesser, Anne Stenersen, and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect," in *Perspectives on Terrorism* 10, no. 6, December 1, 2016, pp. 3-24, URL: www.jstor.org/stable/26297702, accessed at 05 August 2020.

[6] Europol, "European Union Terrorism Situation and Trend Report 2018 (TE SAT 2018)," June 20, 2018, URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018, accessed at 05 August 2020.

[7] Europol, "European Union Terrorism Situation and Trend Report 2019 (TE SAT 2019)", June 27, 2019, URL: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat, accessed at 05 August 2020.

[8] Europol, "European Union Terrorism Situation and Trend Report 2020 (TE SAT 2019)," June 23, 2020, URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020, accessed at 05 August 2020.

[9] Alan M. Dershowitz, *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*, Yale University Press, New Haven, 2002, p. 6.

[10] Radhika Halder, *Understanding Suicide Terrorism*, KW Publishers Pvt Ltd in association with Centre for Air Power Studies, New Delhi, 2019.

[11] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies, Washington, DC, 2002, p. 8, URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, accessed at 05 August 2020.

centre of the jihadi sub-culture. Therefore, the term "Londonistan" was invented to express the recklessness of the British authorities to extremists. In the following years, the jihadi network continued to spread in the UK as well as the rest of Europe, keeping a close connection to the core network in London.[12] Only after the London bombings of July 2005, the United Kingdom drafted the "European Union Counter-Terrorism Strategy", which has been adopted in December 2005. The numerous terrorist attacks that have taken place since then have exposed some shortages in the EU's counter-terrorism policy. However, the biggest deficiency is considered to have been the lack of investment in preventative measures in order to eliminate the possibility of vulnerable individuals to become extremists.[13]

Since 2005, but especially after 2008, jihadis from all over the world demanded another form of jihadism, namely "decentralized jihad", which presumed independently launched attacks in the West.[14] As a consequence, there was an increase in the number of plots directed by single terrorists in Europe who also took advantage of a new form of propaganda, through social media.[15]

Shortly after, the EU counter-terrorism strategy was adopted by the Council in order to fight terrorism globally and provide a safer Europe. The strategy presents four pillars: prevent, protect, pursue, and respond. The prevention of terrorism is the priority of the Council, as it adopted the EU strategy for combating radicalisation and recruitment to terrorism in 2008. This strategy was revised in 2014, with the revised strategy being implemented by the member states later on.[16] As the European states interfered more in the eradication of terrorism in the Muslim world, the number of plots over Europe increased accordingly. According to Nesser, transnational jihadism played a very important role in al-Qaeda's strategy after 2008, shifting from only indiscriminate attacks which were carried through mass-casualty terrorism, to both indiscriminate and discriminate aggressions.[17]

Having the European authorities improved their security measures, al-Qaeda, as well as other new terrorist actors (such as ISIS), adapted their weapons and tactics to withstand the new Western efforts.[18] However, a report made by RAND Corporation's National Defense Research Institute has shown that non-European terrorist organizations do not usually directly recruit European Muslims. The jihadist ideology is spread throughout Europe mostly by radicalising agents that are not formally affiliated with al-Qaeda or other terrorist movements. Even though most of the European based jihadists are self-radicalised individuals, there is a strong connection between them and al-Qaeda or other affiliated organizations, as the former usually tends to follow the latter. This happens because the bigger a group is, the more means it has to provide for more likely successful plots.[19] Therefore, the already-existing counter-terrorism measures proved to be insufficient for Europe, as none of the four already mentioned pillars could successfully work under the new conditions.

---

[12] Petter Nesser, *Islamist Terrorism in Europe*, Hurst & Company, London, 2018, pp. 37-38.
[13] Amanda Paul and Tommaso Virgili, "Three Years after the Brussels Attacks: No Quick Fix to Counter Terrorism and Radicalisation", European Policy Centre, March 20, 2019, URL: https://wms.flexious.be/editor/plugins/imagemanager/content/2140/PDF/2019/pub_9099_3_years_after_brussels_attacks.pdf, accessed at 05 August 2020.
[14] Nesser, *Islamist Terrorism*, p. 56.
[15] Nesser, *Islamist Terrorism*, p. 56.
[16] The Council of the European Union, "EU Counter-Terrorism Strategy," Consilium, October 25, 2018, URL: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/, accessed at 05 August 2020.
[17] Nesser, *Islamist Terrorism*, pp. 56-57.
[18] Nesser, *Islamist Terrorism*, pp. 56-58.
[19] Lorenzo Vidino, "Radicalization, Linkage, and Diversity - Current Trends in Terrorism in Europe," RAND Corporation, July 6, 2011, URL: https://www.rand.org/pubs/occasional_papers/OP333.html, accessed at 05 August 2020.

To protect the citizens and infrastructure, and therefore reduce vulnerability to attacks, the newly revised EU counter-terrorism strategy included several measures: "securing external borders, improving transport security, protecting strategic targets and reducing the vulnerability of critical infrastructure".[20] The "pursue pillar" has been focusing on obstructing the capability of terrorists to plan and organise, as well as bringing the terrorists to justice since 2008. To achieve these objectives, the EU needed to shift its focus on improving both the capabilities of each member state, as well as cooperation and information exchange between police and judicial authorities. Greater attention has also been given to the eradication of terrorist financing through divesting terrorists of their means of support and communication. The fourth pillar accentuates the importance of a quick response after a possible terrorist attack, its objectives being to prepare, manage, and minimise the aftermath of a terrorist attack. For this strategy to work, it needs to operate on a global scale, as the EU's security is closely linked to the situation in other countries. Therefore, in February 2015, the Council emphasized the need for EU's engagement with third world countries on issues regarding security and counter-terrorism.[21]

However, the moment from which awareness was dramatically increased is represented by the 2016 Brussels attacks. Since then, the EU has adopted several measures to address the imminent danger of a terrorist attack. The main fields in which the European Union has shown great progress over time are intelligence sharing, prevention, tackling online radicalisation and straightening ties with partner countries. Many barriers, such as a reluctance for sharing information, have been either removed or, at least, reduced.[22]

2. How the threat of terrorism still affects Europe

The following decade after the Madrid (2004) and London (2005) terrorist attacks registered a continuous decrease in the terrorist activity happening inside Europe. However, since 2014 the number of plots significantly increased. The period between 2015 and 2016 brought an intense fear for Europeans, as the situation seemed unmanageable. After strong measures were implemented, both at the national and the European level, the scenario notably improved. As a result, in the last couple of years, there have been fewer and fewer attacks and casualties. Nevertheless, the fact that the situation improved does not presume that things just 'go back to normal', as they were before the terrorist threat oppressively emerged in Europe. First of all, the Europeans' mindset regarding terrorism changed drastically, as it was not 'a distant matter' that affected only the Middle East anymore, it had a direct effect over Europe. Second, it deepened internalized racism and islamophobia, which also led to many discriminatory laws that were implemented by nationalist governments.

Scholarly works have shown that most of the recent attacks in Europe are caused by "homegrown terrorists", meaning that the perpetrator is leading the attack in his home nation, the victims having the same citizenship as the perpetrator.[23] Scholars argue that the radicalisation of European Muslims is the main cause of "homegrown terrorism", highlighting the strong impact of religious beliefs over easily influenced people.[24] While some scholars argue that the Islamic ideology directly stimulates, in the most extreme cases, the use of

[20] The Council, "EU Counter-Terrorism Strategy."
[21] The Council, "EU Counter-Terrorism Strategy."
[22] Paul and Virgili, "after the Brussels Attacks".
[23] Gary Jackson, *Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security*, Wiley, Hoboken, NJ, 2012, p. 235.
[24] Saifuddin Ahmed and Jörg Matthes, "Media Representation of Muslims and Islam from 2000 to 2015: A Meta-Analysis," in *International Communication Gazette* 79, no. 3, 2017, pp. 219–244.

violence, others claim that radical individuals use the extremist Islamist ideology as a justification for their actions.[25] Despite the clear evidence that neither refugees nor migrants are the key elements behind a terrorist attack, immigrants are treated poorly all over Europe due to fear. Studies show that terrorist attacks cause people to be more reticent about immigrants especially if the terrorist plot happened within their country. However, this reticence is present in the neighbouring countries too, therefore rapidly spreading out across Europe. This way, an indirect consequence of terrorism stands in the feeling of imminent danger which drives individuals into discriminating innocent people, changing irremediably the public opinion on migration.[26]

Another issue that started mainly out from the fear of terrorism, but also from the multiculturalism debate, is the wearing of Muslim veils. Over the last years, many European states decided to restrict or even ban the covering with Islamic face veils, arousing much controversy among the people, even involving the European Court of Human Rights. However, studies have shown that these laws had very limited positive effects on Islamist terrorism in European states. On the contrary, the countries which have successfully enforced veil bans proved to be statistically much more likely to encounter more lethal Islamist terrorist attacks than the states in which such laws do not exist.[27]

The mere fact of terrorism's active existence, even if it is kept under control in Europe, leads to a vicious circle. Terrorist threats in the Middle East, particularly in Iraq and Syria, cause major migration waves in Europe, a fact that force European states into taking extreme measures to please their citizens. This way, terrorist groups perceive the newly taken measures as discriminatory towards their beliefs, focusing their activity on those particular nations that implemented such 'preventive actions'. Besides the extremist Islamist groups that get offended by such actions implemented by the governments, Muslim people could be easily influenced by similar extremist groups under this context, spreading the radicalisation process at a more rapid pace in Europe.

The online world is another troubling weapon for terrorists to spread propaganda and gain support. The online traffic some footage from a terrorist attack makes is inconceivable, all because extremists spread the video or photo materials all over the internet, through every accessible media platform. As a consequence, European countries are fighting to ban any terrorist-related content off the most popular social media platforms. The EU has already proposed such legislation in September 2018 but it is still debated, as the COVID-19 pandemic delayed the discussions. The new law would require the social media platforms to review and subsequently delete any terrorism-related materials in no more than an hour from the moment in which a notice has been issued. Afterwards, the platforms would need to make sure that the deleted content cannot be reuploaded. If a platform fails to comply with the mentioned rules, it will be fined with up to 4 percent of its global annual revenue. Many critics argue that this law would violate the right to freedom of expression, this being one of the main reasons for which the debate is still ongoing. However, in order to stop organizations

[25] Clara Egger and Raùl Magni-Berton, "The Role of Islamist Ideology in Shaping Muslims Believers' Attitudes toward Terrorism: Evidence from Europe", Studies in Conflict & Terrorism, February 20, 2019, URL: https://doi.org/10.1080/1057610X.2019.1571696, accessed at 05 August 2020.
[26] Tobias Böhmelt, Vincenzo Bove and Enzo Nussio, "Can Terrorism Abroad Influence Migration Attitudes at Home?", in *American Journal of Political Science* 64, pp. 437-451, December 2, 2019, URL: https://doi.org/10.1111/ajps.12494, accessed at 05 August 2020.
[27] Nilay Saiya and Stuti Manchanda, "Do burqa bans make us safer? Veil prohibitions and terrorism in Europe", *Journal of European Public Policy*, November 1, 2019, URL: https://doi.org/10.1080/13501763.2019.1681494, accessed at 05 August 2020.

such as ISIS from using popular platforms like Google or Facebook to gain support and radicalise individuals, action must be taken.[28]

3. What is left to do?

Even if the statistics show that the situation improved considerably in Europe, the terrorist threat is not dead. Nowadays Europe is indeed much better prepared to deal with radicalisation and terrorism than it was a few years ago, but it is still not enough. The EU was used to act only as a response to some major crises, while this is not acceptable anymore. There are still many serious challenges in the prevention sector, crucial for assuring that no more innocent lives are lost as a result of terrorism.

One serious challenge that European states, as well as other countries, have to deal with is what to do with the captured foreign fighters. Prosecutions without specific legal evidence are almost impossible, taking into consideration the inaccuracy of the events happening on the battlefield. Therefore, several potential criminals could get away with horrendous felonies, while war heroes could easily be mistaken for culprits. Another great challenge that raised the concern of some EU member states, like France and Belgium, is the radicalisation process taking place in European prisons. The 2018 terrorist attacks from Liège and Strasbourg validate the relevance of the issue, as both the attacks were carried out by individuals radicalised in prison. Additional attention from the EU to this issue is crucial so that these tragic events will not occur again. Finally, the failure to provide an exact definition of terrorism is a big impediment to the eradication of terrorist acts. If the terms "radical" and "terrorism" have no definite meaning, there is no clarity on how to fight this phenomenon and what are the lengths to which one can fight it.[29]

The future mission of the EU should focus on convincing its member states that the implementation of supranational counter-terrorism policies is mandatory in today's situation and common ground on defence strategies should be achieved. As the capacity to guarantee national security is the core of states' sovereignty, member states are often reluctant to any supranational policy regarding their security. However, it has been proven that member states can act quickly if they perceive that it is to their best interest to integrate counter-terrorism policies. The 9/11 attack demonstrated that in the face of high-profile events member states are determined to act decisively.[30] Therefore, EU integration plays a major role in international security, in particular in combating terrorism. It is impossible to abolish this impending threat without common policies and global cooperation.

Conclusions

Since the end of World War II, extremist groups have carried out numerous acts of violence in Europe in the pursuit of political and religious objectives, using multiple tactics. Even if terrorist attacks inside Europe had reduced significantly, radicalisation is still a very important, global problem that should not be neglected. The Council has made considerable progress in combating and preventing terrorism, starting with the 1977 European Convention

[28] Jon Porter, "Upload Filters and One-Hour Takedowns: the EU's Latest Fight against Terrorism Online, Explained," The Verge, March 21, 2019, URL: https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu, accessed at 05 August 2020.
[29] Paul and Virgili, "after the Brussels Attacks".
[30] Christopher Wieczorek, "Improving Counter-Terrorism Policy Integration in the European Union: An Analysis", Carleton Review of International Affairs, July 5, 2018, URL: https://doi.org/10.22215/cria.v5i0.1320, accessed at 05 August 2020.

on the Suppression of Terrorism and culminating with the 2005 European Union Counter-Terrorism Strategy. However, there is still plenty of room for improvement, as the EU is still struggling with major discrepancies.

As it has been mentioned before, the decreasing numbers of successful attacks and victims in Europe should not lead to a complete relaxation of the preventive and defensive measures. If the threat of terrorism is neglected, it will rise again more powerful than before, given the various means that extremists can use nowadays. There are still several shortcomings that the European states must urgently address to be prepared for other plots. At the same time, people should be educated more on this matter, so anyone could clearly understand why extremism is so dangerous. Prisons represent the most suitable places for radicalisation, as people turn to extremist groups to find a purpose. Better education in prisons could largely diminish terrorist threats and could also open new opportunities for individuals which lost their path.

Every big problem that a nation experiences come from a lack of safety felt by its citizens. A state's biggest responsibility is to assure its people a safe environment to live in. When the state cannot fulfil its obligation towards its citizens, they start being fearful and search for places where they can live in safety. This is the point from which immigration starts, leading to other challenges experienced by distant nations, as the European migrant crisis was. Therefore, even if the number of terrorist plots is decreasing in Europe, the eradication of terrorism should still be a priority for the European law-makers as it has direct consequences over all the European nations.

BIBLIOGRAPHY:

1. ***, *EU Counter-Terrorism Strategy*, EU Consilium, October 25, 2018. URL: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/
2. ***, Rep. *European Union Terrorism Situation and Trend Report 2019 (TE SAT 2019)*, June 27, 2019, URL: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat
3. ***, Rep. *European Union Terrorism Situation and Trend Report 2018 (TE SAT 2018)*, June 20, 2018, URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018
4. ***, Rep. *European Union Terrorism Situation and Trend Report 2020 (TE SAT 2020)*, June 23, 2020, URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020
5. AMANDA, Paul, and VIRGILI, Tommaso, Rep. *Three Years after the Brussels Attacks: No Quick Fix to Counter Terrorism and Radicalisation*, European Policy Centre, March 20, 2019, URL:https://wms.flexious.be/editor/plugins/imagemanager/content/2140/PDF/2019/pub_9099_3_years_after_brussels_attacks. pdf.
6. DERSHOWITZ, Alan M, *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*, New Haven, Yale University Press, 2002.
7. EGGER, Clara, and Raùl MAGNI-BERTON, "The Role of Islamist Ideology in Shaping Muslims Believers' Attitudes toward Terrorism: Evidence from Europe", *Studies in Conflict & Terrorism*, February 20, 2019, URL: https://doi.org/10.1080/1057610x.2019.1571696
8. HALDER, Radhika, *Understanding Suicide Terrorism*, New Delhi, KW Publishers Pvt Ltd in association with Centre for Air Power Studies, 2019.
9. HOFFMAN, Bruce, *Inside Terrorism*, New York, Columbia University Press, 2006.
10. JACKSON, Gary, *Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security*, Hoboken, NJ: Wiley, 2012.

11. JONES, David Martin; SCHULTE, Paul; UNGERER, Carl and SMITH. M.L.R., *Handbook of Terrorism and Counter Terrorism Post 9/11*, Cheltenham, UK, Edward Elgar Publishing, 2019.
12. LEWIS, James Andrew, Center for Strategic and International Studies, Washington DC, 2002, URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
13. MILLER, Erin; LAFREE, Gary and DUGAN Laura, "Terrorism Fatalities", 2018, URL: https://www.start.umd.edu/gtd/.
14. NESSER, Petter, *Islamist Terrorism in Europe*, Hurst & Company, London, 2018.
15. NESSER, Petter; STERNERSEN, Anne and OFTEDAL Emilie, "Jihadi Terrorism in Europe: The IS-Effect", *Perspectives on Terrorism* 10, no. 6, December 1, 2016, URL: www.jstor.org/stable/26297702.
16. NILAY, Saiya and MANCHANDA, Stuti, "Do Burqa Bans Make Us Safer? Veil Prohibitions and Terrorism in Europe", *Journal of European Public Policy*, November 1, 2019, URL: https://doi.org/10.1080/13501763.2019.1681494
17. PORTER, Jon, "Upload Filters and One-Hour Takedowns: the EU's Latest Fight against Terrorism Online, Explained", *The Verge*, March 21, 2019, URL: https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu
18. SAIFUDDIN, Ahmed, and MATTHES, Jörg "Media Representation of Muslims and Islam from 2000 to 2015: A Meta-Analysis", *International Communication Gazette 79*, no. 3, 2017.
19. VIDINO, Lorenzo, "Radicalization, Linkage, and Diversity - Current Trends in Terrorism in Europe", RAND Corporation, July 6, 2011, URL: https://www.rand.org/pubs/occasional_papers/OP333.html.
20. VIDINO, Lorenzo, "Radicalization, Linkage, and Diversity: Current Trends in Terrorism in Europe" *Psyc EXTRA Dataset*, July 6, 2011, URL: https://doi.org/10.1037/e525772012-001
21. WIECZOREK, Christopher, "Improving Counter-Terrorism Policy Integration in the European Union: An Analysis", *Carleton Review of International Affairs* 5, July 5, 2018, URL: https://doi.org/10.22215/cria.v5i0.1320

INFLUENCE OF CYBER THREATS ON THE AIR FORCE COMMAND AND CONTROL SYSTEM

Vasile-Cristian ONESIMIUC
Ph.D. Student, "Carol I" National Defense University, Bucharest, Romania.
E-mail: ovcairforce@yahoo.ca

Sorin TOPOR, Ph.D.
Capt. (N), Professor "Carol I" National Defense University, Bucharest, Romania.
E-mail: sorin_topor@yahoo.com

Abstract: *Cyber threats are found in all domains, both civil, and military, but their effects are more important for the Air Forces. Cyber threats have dual functions, that is, as expected, they can have negative effects, but, surprisingly, Air Forces could use the negative effects of cyber threats for the support of its own missions. From the cyber security point of view, being aware of its own limitations as well as those of the adversary's is never completed, but it represents one of the elements that can bring about the success for the Air Forces mission, whichever that may be: defending its own capabilities or attacking the enemy. The only certainty within this process is the increase in future influence over the Air Force actions.*

Keywords: *Air Forces; cyber threat; risks; command and control.*

The year 2016 brought recognition[1] for cyberspace as military operational domain where NATO has to defend itself as efficient as possible in the air, on the ground and on the sea. In this way, the interest showed by military commanders for this new domain has grown, and they acknowledged the importance of integrating cyber actions into conventional military operations. This increased interest has led to the adaptation of performed air forces operations, both domains being interdependent, cyber operations had to support the act of obtaining freedom of maneuvers for one's own forces. Acknowledging cyber space as an operative domain equally important as those already existing at NATO level, has done nothing but to recognize the importance of some actions that have already been executed at the level of the armed forces of some states, actions in cyber space having been already used for the increase or decrease of the combative capacity of air forces, by executing offensive and defensive cyber operations, as the case may be.

Air force importance within armed forces is evidenced by their intense use in military conflicts, the beginning of the hostilities being marked by execution of an air campaign necessary for earning air superiority and fulfillment of conditions as required for the performance of operations by all other forces. Under these circumstances, where the actions of the air forces have a high importance, executing some cyber actions becomes highly probable for disturbing actions or even eliminating from the battle the air forces assets.

[1] ***, NATO *Warsaw Summit Communique*, 2016, para. 70, URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm, accessed on 28.08.2020.

For example, in 2007, within Orchard[2] operation, where Israeli air forces executed bombing missions over some targets located in Syria, there were information on performing some offensive cyber actions for taking out of the battle of air defense systems found on the flight path used for the bombing missions. It is worth mentioning that these cyber actions are executed secretly and usually information on the success of a cyber operation is revealed only when deemed as improbable for the cyber weapons already used to be used later on, or for acknowledging a certain level of capabilities as detained by a cyber actor, with all corresponding risks.

In our opinion, from the point of view of the Israeli command and control system, evaluation of the situation has contributed to the need to use offensive cyber actions in support of aircrafts missions, for cyber penetrating the adversary's networks, being preferred to the use of any other combat assets. It is very much possible that, for 2007, the state of Israel had the necessary means to know the real possibilities of the sensors used by Syrian systems and to execute some cyber actions to alter the air image shown at the level of command centers of air defense.

From the point of view of the command and control system used by the Syrian Air Forces, those cyber actions which were probably performed, have been executed under a threshold which would have allowed the detection of the attack (the cyber-attack was, most likely, very well calibrated so as to maintain for the targeted systems the feeling of normality, operationally speaking) and benefitted extra from the element of surprise, considering that, at the respective moment, the cyber activities executed by Israel in cooperation with the United States of America related to the Stuxnet virus[3] were not known.

It is our opinion that technological advancement of the Israeli air forces did not ensure total elimination of the risks associated to the execution of bombing missions. Where the Israeli commanders knew the limits of their own systems, both at cyber level, and for the air means, the cyber-attack should be precisely executed, for a limited period of time, but with effects close to maximum, to allow bombing the targeted facilities. The Israeli evaluation and decision making process has proven superior to the Syrian one, and consequently the success of the mission was mostly determined by the audacity of the executed attack. Location of the bombed target deep in the Syrian territory and the powerful Syrian air defense system appeared to be elements strong enough to discourage, from the very beginning, a potential attacker.

Closer to present times, the security situation in Ukraine, following the currently on-going conflict, does present an interest for the cyber actions over the air forces. In this context, prior Russian concerns for offensive cyber actions are important to mention, among which there also cyber actions are performed during the war in Georgia in 2008.

From the point of view of cyber actions, the Georgian conflict became known as the first evidenced case where conventional military actions of a state against another were preceded by offensive cyber operations[4] performed in support of military actions. Seeing things from this perspective, the conflict from 2008 represented a training stage for the actions performed in Ukraine. Cyber-attacks carried on in Georgia were meant for priory established targets. Cyber weapons, which at the time did suggest a high level of knowledge of the

[2] A. Pfeffer, *Operation Orchard: how Israeli jets flew at low altitude to avoid detection in Syria*, 2018, URL: https://www.thejc.com/news/israel/operation-orchard-nuclear-syria-strike-how-israeli-jets-flew-at-low-altitude-to-avoid-detection-1.461050, accessed on 27.03.2020.

[3] ***, *Virusul Stuxnet, proiect americano-israelian pentru sabotarea programului nuclear iranian*, 2011, URL: https://www.mediafax.ro/externe/virusul-stuxnet-proiect-americano-israelian-pentru-sabotarea-programului-nuclear-iranian-7893704, accessed on 28.08.2020.

[4] ***, *The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict*, 2012, URL: https:// www.afcea.org /committees/cyber/documents/therusso-georgianwar2008.pdf, p. 13, accessed on 29.08.2020.

computer programs and systems used by Georgian authorities, were used and their actions disturbed the Georgian military control and command system[5].

It is also very important to analyze and evaluate the already known actions as carried out by a nation state cyber actor, in order to be able to extract information to use within the decision-making process for performing some missions by the air forces. Unfortunately, this thing is not so easy to achieve, as synthetically put by a Ukrainian military commander, Colonel Andrey Lesenko[6] with respect to Russia's aggression over Ukraine: *"*We often exercised and deployed our joint manoeuver forces to operate in a contested warfighting environment. So, we thought we were postured, prepared and ready for any major Russian incursions. Critically however, we had failed to properly exercise, and therefore truly understand, the impact of losing control of Defense Information and communications technology (ICT) networks, systems and data links critical to the command, coordination and conduct of maneuver warfare. As a result, the subsequent speed and synchronicity in which the Russians orchestrated and delivered the cyber-attacks within kinetic and non-kinetic joint fires was overwhelming and catastrophic. It left us on the canvas: deaf, dumb and blind – we were essentially rendered combat ineffective in 118 minutes!"

In our view, the Ukrainian commander presented in a concise manner how a wrong evaluation of threats and associated risks has led to the success of the offensive cyber actions performed by the adversary, the Ukrainian commanders being totally outweighed by the way Russia used, in a conjugated manner, cyber actions to support classical military actions. It is obvious that the process of gathering information on the adversary could offer some data on offensive cyber capabilities of the adversary, but Ukrainian commanders did fail to understand their effects on their own command and control systems. The technological advancement the attacker benefitted from allowed total surprise of Ukrainians, the fact that they did not manage to foresee the integration of cyber capabilities into conventional military actions, is due to the element of novelty, but, most likely, to the lack of adequate means to respond to new threats, from the Ukrainian side.

Moreover, as seen from the Ukrainian commander side, the training level with respect to joint action level reached by Ukrainian forces was considered satisfactory, ensuring a high level of trust, but it has proved very different from the reality. We should not overlook the fact that Russia was able to freely access the Ukrainian equipment because they had been built in the former Soviet Union, and thus, knowing in detail the way the networks[7] used by Ukrainians could be broken into.

Seeing things from the attacker's side, the Russian command and control system applied the lessons learned during 2008 conflict in Georgia, the cyber-attacks did not leave traces to incriminate them directly for the performance of such attacks. Russian actions within cyberspace performed in Ukraine have, yet again, proven the advantage of the offensive action over the defensive ones, the cyber-attacks being able to reach their objective to disturb and even to make impossible for the envisaged targets to carry on their activities[8].

Understanding cyber domain is the responsibility of the command authority, considering that it touches upon all other components of modern war. The revolution caused by using information and computers in support of military actions has changed the way

[5] Lomidze, I., *Cyber Attacks against Georgia*, 2011, URL: https://dea.gov.ge/uploads /GITI%202011 /GITI2011_3.pdf, accessed on 29.08.2020.
[6] Wilson, G., *Planning and Liaison, Electronic warfare -threat from a command post perspective*, 2020, URL: https://cove.army.gov.au/article/electronic-warfare-threat-command-post-perspective, accessed on 28.08.2020.
[7] ***, "The Ukrainian crisis – a cyber warfare battlefield", *INSS*, 2014, URL: https://defense-update.com/ 20140405_ukrainian-crisis-cyber-warfare-battlefield.html, accessed on 30.08.2020.
[8] S.A. Medvedev, *Offense-Defense Theory analysis of Russian cyber capability*, Naval Postgraduate School Monterey, California, 2015, p. 42, URL: https://core.ac.uk/download/pdf/36737355.pdf, accessed on 30.08.2020.

modern war is being conducted. In order to be able to use the cyber capabilities towards their maximum level, commanders need to have a higher knowledge on offensive and defensive cyber operations, both strategically and tactically.

As for the air force commanders, they have to be the best managers, to be able to understand the characteristics of all categories of forces and specialties under their command, all these to efficiently manage and with maximum results in battle. Similarly, for the cyber domain, an air force commander has to be able to understand the details of specific operations, such as role and place of cyber defense specialists, in order to jointly use the capabilities found at their disposal during the missions they lead, leaving the execution part to those who actually have to fight.

From the point of view of air means, they evolve both in air domain, as well as in the cyber one, and, consequently there becomes absolutely necessary the dual approach of the two domains. The learning process, following which commanders reach a high level of expertise, equally requires time and training. From this point of view, the need for specific training of air force personnel poses some problems regarding the compatibility of professional training in aeronautics and cyber area.

Training to become a pilot does not exclude the possibility of getting training in cyber security. However, this niched domain requires, at least until reaching a high level of expertise, choosing a clear professional direction as compared to others. There cannot be done a joint type of training without having been well trained in a certain weapon and with a certain specialization. It is only with that approach, that we can assess the functional relationships becomes a relationship of an optimal command and control system.

Air Force command and control system[9] is made up of the command and control structures, the command chain and the support system. For the Romanian Air Forces, the command and control structures are Air Force General Staff and unit headquarters under its command, while the command chain is formed by the commanders within those units. Through these structures, there are being attained the principle of command unity, centralized planning and de-centralized execution, the unity within military actions, as well as reducing the time required for making a decision.

The support system is formed by sub-systems of information, communications, informatics, air navigation and identification, integrated logistical support, operation centers, command posts and procedures. Air operations are performed considering a few principles, among which there are centralized control and de-centralized execution, priority of the offensive actions, informational superiority and synergy of effects; using these principles within the command and control system of air forces allows the influence of the cyber threats of the adversary.

Romania's cyber security strategy defines cyber threat as being a *"circumstance or event which constitutes a potential danger to cyber security*[10]". This potential danger to cyber security for the command and control system of the air forces, most likely, is the result of performed actions of a nation state actor or other actor which is actively receiving support from a state in carrying out cyber operations, those actors aiming, probably, to perform a series of activities, beginning with the most simple ones – identifying and mapping the used networks, espionage activities, up to performance of complex cyber-attacks. Therefore, the threat and the execution location of the attack (reaching the desired objectives) are very important from the attacker's point of view. The analysis done by the Romanian Intelligence

[9] ***, *Doctrina pentru operații a Forțelor Aeriene*, București, 2016, pp. 27-29.
[10] ***, *Cyber security strategy of Romania*, 2013, section 3, para. 6, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania, accessed on 20.08.2020.

Service points out that nation-state cyber actors continue to represent „*the main form of threat on Romania's cyber security, being mostly directed against IT&C infrastructures with critical nuances to national security*[11]"

From the point of view of the one under attack, the command and control system most likely will react to actions performed in the cyber space, under one basic condition: that adversary's actions be intercepted and evaluated from the early stages of developing. For air force commanders is easy to evaluate the effects of cyber-attacks when they produce damages that can be quantified and are visible. The troubles begin when such effects are not visible for the attacked one, and it does not apply immediate and efficient measure to counterattack them.

For a state with proven credible military superiority, it is most likely that an opponent will look to develop its cyber capabilities to efficiently counterattack the lack of classical military assets. This does not automatically turn into advanced cyber capabilities, but in cyber space the initiative rests with the attacker, whereas availability of a various cyber arsenal offers enough possibilities to act for breaking through cyber defense of the adversary. It is worth mentioning that „*63% of all security incidents discovered by Cisco Stealthwatch have been found to be within encrypted traffic*[12]" according to the data reported by the Romanian Intelligence Service; at first sight, powerful cyber actors have available means to ensure initiative for the attacker.

Air forces command and control systems integrate forces and means available within a complex system, where a lot of interdependencies appear between its constituent elements, air means, air defense systems, radar systems, research, surveillance, logistical facilities or maintenance etc., all being interconnected to facilities belonging to cyber space. Thus, cyber threats for the air forces should be evaluated in this context drown up by sub-systems. It is obvious that the task of the one defending itself is almost impossible; it is unable to ensure the same level of cyber security for all the equipment in the network.

The command and control system must exceed time and resources limitations to manage the offensive and defensive cyber means found at its disposal, so as to secure the domains being considered essential for the completion of mission, while, at the same time, to execute its own offensive cyber actions. It is obvious the adversary's will to perform cyber-attacks on air forces with the purpose of causing trouble to its acting possibilities, or, at least, to carry on better knowledge of opponent's used systems.

It is no longer about whether there will be attacks or not, but rather when they will be detected, preferably before they produce negative effects[13]. Therefore, the command and control systems, cyber threats will have to be considered very seriously, but there will be need to reach a balance between measures to ensure cyber security and control of bureaucracy induced by new restrictions being introduced, which have the potential to slow down the speed for making decisions within air forces.

Based on the increasing complexity of executed and identified cyber-attacks, on the development of technology used in the air force, we can say that the number of cyber-attacks detected is much lower than those actually executed, consequently the possibility of a cyber actor to perform hostile cyber actions over its adversary air force systems is high, also in peacetime.

---

[11] ***, *Buletin Cyberint*, semester 1, 2020, p. 3, URL: https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2020.pdf, accessed on 28.08.2020.
[12] *Ibidem*, p. 23.
[13]***, *Aviation Cyber Security Strategy*, para. 41, p. 23, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726561/aviation-cyber-security-strategy.pdf, accessed on 26.08.2020.

The aircrafts are dependent on support systems, most of them are controlled through cyberspace. It is obvious that the process of assessing the resilience of air operations must take into account cyber vulnerabilities for those systems.

The effects obtained on the equipment by performing cyber operations are both in the virtual, and in the physical field, but we must take into account effects on the psychological part, how these effects can influence staff morale. It is well known that flight crews have a high confidence in the ability of their aircraft, due to the combination of factors represented by personal training, maintenance of the aircraft, knowledge of the aircraft and manner they react in certain situations.

Moreover, cyber operations executed by state cyber actors are not disclosed, their execution and the resulting effects are kept secret, so that they can be exploited in the place and at the time desired by the attacker. The vast majority of cyber operations used in the armed forces have a certain degree of classification and are not available to the general public.

The actual possibility to penetrate the cyber defense of the desired target has direct implications on cyber security in the air force, the apparent normality induced by the lack of detection of hostile cyber activities can inspire a perception of false security to targets. Once the opponent decides to use its superior cyber capabilities, it will have freedom of maneuver and there is the real possibility of removing the targeted air force means from combat.

Cyber weapons are designed and used for carrying out specialized cyber-attacks, on well-defined targets, which require a certain mode of action to cause the desired effects. The main difference from other military domains is that effects in cyberspace can be obtained in a very short time, within seconds. Cyber operations have shortened the time between decision making and effects of operations, which requires flexibility in command and control[14]. As a result, decision-making and execution of actions in cyberspace in response to an opponent's attack require fast reactions, which must be taken at different levels of the control chain. More important, the speed of decision-making can make the difference between a successful operation and a total disaster.

In order to carry out a successful cyber-attack or for a potential adversary to present credible cyber threats to the air force assets, it is necessary to possess an advanced level of development of offensive cyber capabilities. Moreover, the high speed of execution of attacks in cyberspace, given its execution at a high level of complexity, can lead to an incorrect assessment of the level of cyber threat by the target. From the point of view of the command and control system, the incorrect assessment of the level of the cyber threat leads to a series of subsequent actions that can prove disastrous for the air forces.

The characteristics of cyber actions, the difficulties concerning the attack attribution, the automation and the connectivity of the systems make the current security environment more and more contested, while the cyber threats can lead to uncertainties regarding the level of development of nation state cyber actors.

Conclusions

It is our opinion that, at the present moment, the air force command and control system in place is aware of the level of risks and threats coming from cyberspace. A very important aspect regarding the visibility of cyber-attacks carried out so far, is that just a small part of it has been analyzed and, from them, elements of interest are being extracted on how they were used and what effects were obtained from the execution of attacks. However,

[14] C. Stallard, *At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force*, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, 2011, pp. 15-17, URL: https://www.hsdl.org/?view&did=800524, accessed on 26.08.2020.

commanders noted the potential of offensive and defensive cyber operations and the fact that their integration into traditional military operations could be the key to the success of their missions.

Cyber operation executed in support of air forces are conducted in advance, most of the time, way ahead before the targeted system could detect the presence of the adversary inside one's own systems. For the air force command and control systems, the extended possibilities of executed cyber-attack by using superior cyber offensive capabilities should not lead to cessation of measure implemented to ensure the cyber security of their own systems. Many unknowns associated with cyber actions lead to a great deal of mistrust, both in the capabilities of one's own systems and those of the adversary, but we can certainly say that cyber actions will play an increasingly important role in future air force actions.

In our opinion, cyber threats will influence future air forces operations and, at the same time, the command and control systems by the following:

- cyber operations will be carried out long time before the execution of conventional military actions, in order to obtain information on the adversary, information that may prove very important for the decision-making process before and throughout the execution of air force missions;
- the possibility of disrupting or modelling very quickly the actions performed by an adversary, due to the very high speed of cyber-attacks execution;
- cyber operations would prove to be one of the few measures to respond to actions performed by an adversary, with cyber actions offering reversible and transient methods of action against it;
- the possibilities for action in the cyberspace will determine commanders to pay more attention to indicators that may signal a possible interference in their own networks, by allocating specialized teams and resources to a higher level than at present;
- technological advance will create the conditions for a much faster development of cyber capabilities compared to the time of development and putting into operation of the conventional armament systems.

BIBLIOGRAPHY:

1. ***, *Aviation Cyber Security Strategy*, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726561/aviation-cyber-security-strategy.pdf
2. ***, *Buletin Cyberint, semester 1*, 2020, URL: https://www.sri.ro/assets/files/publicatii/ buletin-cyber-sem-1-2020.pdf
3. ***, *Cyber security strategy of Romania*, 2013, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania
4. ***, *Doctrina pentru operații a Forțelor Aeriene* (In English: Air Forces Doctrine for operation), Bucharest, 2016.
5. ***, *NATO Warsaw Summit Communique*, 2016, URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm
6. ***, *The Russo-Georgian War 2008: The Role of the cyber-attacks in the conflict*, 2012, URL: https://www.afcea.org/committees/cyber/documents/therusso-georgianwar 2008.pdf
7. ***, *The Ukrainian crisis – a cyber warfare battlefield, INSS*, 2014, URL: https://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html
8. ***, *Virusul Stuxnet, proiect americano-israelian pentru sabotarea programului nuclear iranian*, 2011, URL: https://www.mediafax.ro/externe/virusul-stuxnet-proiect-americano-israelian-pentru-sabotarea-programului-nuclear-iranian-7893704

9. LOMIDZE, I., *Cyber Attacks against Georgia*, 2011, URL: https://dea. gov.ge/uploads /GITI%202011/GITI2011_3.pdf
10. MEDVEDEV, S.A., *Offense-Defense Theory analysis of Russian cyber capability*, 2015, Naval Postgraduate School Monterey, California, URL: https://core.ac.uk/ download/pdf/ 36737355.pdf.
11. PFEFFER, A., *Operation Orchard: how Israeli jets flew at low altitude to avoid detection in Syria*, 2018, URL: https://www.thejc.com/news/israel/operation-orchard-nuclear-syria-strike-how-israeli-jets-flew-at-low-altitude-to-avoid-detection-1.461050
12. STALLARD, C., *At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force*, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, 2011, URL: https://www.hsdl.org/? view&did=800524
13. WILSON, G., *Planning and Liaison, Electronic warfare -threat from a command post perspective*, 2020, URL: https://cove.army.gov.au/article/electronic-warfare-threat-command-post-perspective

ADJUSTMENT OF AIR POWER TO CHALLENGES RAISED BY CYBER OPERATIONS

Vasile-Cristian ONESIMIUC
PhD Student, "Carol I" National Defense University, Bucharest, Romania.
E-mail: ovcairforce@yahoo.ca

Sorin TOPOR, Ph.D.
Capt. (N), Professor "Carol I" National Defense University, Bucharest, Romania.
E-mail: sorin_topor@yahoo.com

***Abstract**: Innovation and digital technologies have an even greater influence on the development and growth of the air power efficiency. Cyber operations are more and more visible and therefore presented as being part of normality. Upon state level, air force can no longer ignore this reality and has to take active measures to adapt to the new state of normality. Adaptation of the air power to the challenges raised by cyber operations is a lengthy process, which develops continuously and that shall cause additional consumption of means and resources that would usually have been allocated to other activities. However, provided the adaption of the air power to the new reality becomes impossible, then it will, unavoidably, lead to its transformation into a paper tiger.*

***Keywords:** Air Power; mission; cyber operations; adaptation; risk; security environment.*

Innovation and technological development have a very important role to play both in everyday life, and especially in state of the art technologies, such as air force. Air power[1] comprises to all air means of a state that are used for military purposes, it requires the presence and the development of air forces able to perform missions in all situations, so as to discourage, limit or prohibit actions form an adversary. Beginning with the early stages of aeronautics, technological advancement[2] from the civil state-owned sector turned into military advantage, through using it to develop modern military air assets and facilities to ensure the well-functioning of such modern equipment. Bringing this modern equipment within conflicts has led to new technological leaps in aeronautics, development and innovation of aeronautics having been considered as priority and thus being able to receive important funding for research and innovation. Such progress has brought about a dual system, where technical achievements from the civil domain were integrated within the military, but, at the same time, there was a technology transfer from the bombing aircrafts to commercial aircraft. If, on one hand, during a conflict, there is no argue to support the need to allocate funds for development and upgrade of aircrafts used by the air forces, due to evident realities and direct threat onto the state, in times of peace, on the other hand, the need to allocate important funds to the area of research and development in the field of aeronautics is very likely an argued one and, in most cases, no funds is allotted.

[1] ***, *F.A.-1 – Doctrina pentru operații a Forțelor aeriene*, București, 2016, p. 13.
[2] K.L. Best, J. Schmid, S. Tierney, J. Awan, N.M. Beyene, M.A. Holliday, R. Khan, K. Lee, *How to analyze the cyber threat from drones*, RAND Corporation, 2020, p. 5, URL: https://www.rand.org/pubs/research reports/RR2972.html, accessed on 23.08.2020.

Development of air forces has continued to be a mixture between civil and military research, and aviation has turned into a system of interconnected sub-system[3], digital data and information becoming the bind of such a system which should work properly in both everyday operations, and especially in those taking place within media that are challenged with respect to safety and security.

The evolution of this interconnected system brought obvious benefits to aircrafts performances, to airport facilities, and, generally speaking, to the entire activity carried on in civil and military aeronautics. Thus, aircrafts have begun to include more and more technology, the aerodynamic performances have exceeded any prior limits. At the same time, such massive technological intake determined a raise in the dependency degree to computing systems found on-board, which are meant to ensure the capacity to fly for the aircraft, but deficiencies to such computing systems which ensured aircraft stability could, very easily, determine a crash. Technology led to aircrafts that are unstable from an aerodynamic point of view, with forms specifically designed for a certain type of missions, such is, for example, the case of aircraft F-117 Nighthawk[4], with surfaces optimized for radar waves' reflection. This aircraft has a completely computerized flight management system, the flying mission is loaded into the on-board system of the aircraft, and thus it is capable to perform the flight trajectory until the proximity of the target. Moreover, the recording systems found on-board, by recording the impact of the ammunition launched over the target can evaluate the effects of the bombing in real time.

This evolution has brought not only benefits, but, alongside, there have been identified threats that, until then, were non-existent or rather not known and not evaluated. The trend for aeronautics especially to ensuring aeronautical safety for aircrafts contributed to another secondary set of issues, also important financial resources consumers, such as ensuring cybersecurity within the air forces.

Air forces are designed to perform allocated missions both in times of peace, but also in times of crises and war. Cyber space, having been defined[5] as „*virtual environment generated by cyber infrastructure, including content information processed, stored or transmitted, as well as actions taken by users in this*" represents a very important domain for the air forces, considering that, essentially, activities performed by the them are based on interconnection and transmission of data and information necessary for aeronautical activities. Cyber security, defined[6] as „*normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation in electronic information, resources and public or private services, in cyberspace. Proactive and reactive measures may include political, concepts, standards and guidelines for security, risk management, and training awareness activities, implement engineering solutions to protect cyber infrastructure, management identity and management consequence*" has grown in importance, but has not been regarded as an equally important objective to be ensured such as aeronautical safety. Aeronautical safety, from a cyber security point, has to consider those interactions which follow a cyber-attack, because they could be a potential

[3] ***, *System-of-systems notion of cybersecurity in aviation*, International Civil Aviation Organization, Thirteenth Air Navigation Conference, Canada, 2018, p.2, URL: https://www.icao.int/Meetings /anconf13/Documents/WP/wp_270_en.pdf, accessed on 20.08.2020.
[4] ***, *F-117A Nighthawk Stealth Fighter*, URL: https://www.airforce-technology.com/projects/f117/, accessed on 23.08.2020.
[5] ***, *Cyber security strategy of Romania*, 2013, section 3, paragraph 2, URL: https://www.enisa. europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/ strategies/cyber-security-strategy-in-romania, accessed on 20.08.2020.
[6] *Ibidem*, section 3, para. 3, accessed on 20.08.2020.

cause of errors or defects that, in turn, may jeopardize aircraft flights and established safety limits.

Cyber security strategy defines cyber threat[7] as being „*circumstance or event which constitutes a potential danger to cyber security*", whereas security risk[8] in cyberspace is defined, by the same strategy as „*the likelihood that a threat will materialize, exploiting a specific cyber infrastructure vulnerability*". Cyber threats, by exploiting current human, technical or procedural vulnerabilities of the system, can turn up as cyber-attacks of critical infrastructures and cyber espionage. Moreover, from the point of view of the actors performing attacks within cyber space, there is no discrimination between civil or military targets, the objectives being preventing normal activities or even shutting down aeronautical activities. Cyber threats completed the specter of the already existing threats on air forces, raising the risk level, even if air forces are designed to operate and perform flying missions within contested airspace.

It is important to underline that the system of individual sub-systems has to operate in a conjugated, unified manner, as an issue of a sub-system could propagate to adjacent/ neighboring systems in direct connection or which at first sight do not appear having direct connection. Aircraft dependency to an airfield for performing flights has attracted the attention of cyber actors on civil and military airport facilities, thus cyber-attacks on those facilities could affect aeronautical activities as performed by the air forces.

A cyber-attack over an aircraft in flight has, at least on first assessment, a high level of difficulty. Consequently, cyber actors evaluated the methods by which similar results could be obtained. By executing some indirect cyber action, such as attack on airport facility, cyber actors aimed to determine the impossibility to perform flying missions by the air forces targeted.

Even with a pretty detailed analysis of this system of sub-systems in aeronautics, the complex connections within cyber space, as well as the limited ability to understand the possible connections between the sub-systems, can determine the appearance of breaches in the security system for the cyber actors to exploit in order to perform a cyber-attack.

Considering that cyber threats are being scrutinized by the competent authorities in the field, so that active measure are being taken to grow and maintain cyber security within the air forces, it follows that performing a successful cyber-attack belongs in most cases to state cyber actors which are supported by a certain state. The reason behind the attacks, the access to state of the art technologies, the high-qualified personnel, the important material resources necessary to execute cyber-attacks and last, but not least, the prolonged time interval, lead to the idea that behind cyber-attacks performed over important targets of the air forces, there are state cyber actors.

The impact over the air forces of the cyber actors' actions is difficult to evaluate before the actual performance of the cyber-attack. Due to their nature and target objectives, hostile cyber actions are carried on in secrecy, not to warn the attacked targets and to ensure success for the future offensive cyber operations. A state cyber actor that aims for long-term objectives, with patience and provided it has access to state of the art technologies, could perform hostile cyber actions which fall under the detection level of the cyber security system implemented within the air forces. Efficient calibration of actions, through taking apparently small unconnected steps, are usually not monitored by specialists in cyber defense, or, even if they are detected, special attention is not given, and this is so because of various reasons, such as lack of training for the personnel or lack of understanding of the destructive potential of detected cyber actions.

[7] *Ibidem*, section 3, para. 6, accessed on 20.08.2020.
[8] *Ibidem*, section 3, para. 13, accessed on 20.08.2020.

Cyber security in the air forces should be regarded from the perspective of defender, as well as from the attacker's perspective. The defender may feel that is impossible to ensure the cyber protection of all objectives under its responsibility; a question so arises: what are the really critical objectives that need to be protected and how such a protection should be done. Uncertainties cannot totally be excluded, so the defender may run the risk of under evaluating the importance of a certain objective, considering the less obvious links between the sub-systems. Similarly, one should not overlook the fact that actions for ensuring cyber security have to allow ensuring aeronautical safety. Safety changes in aeronautics are quite slow, even after aviation catastrophes caused by clearly identified causes, the recommendations which ensure the raise in aeronautical safety level could not have been implemented overnight. Such implementation is a process which requires time, it is necessary to run a deep analysis for determining the possible links that may affect aeronautical safety and, thus, implicitly, imperil the performance of air forces' missions.

The cyber actor executing the cyber-attack has the possibility to choose the time and location to perform the attack, the way of attacking the target, as well as the forces and the means considered necessary to fulfill the targeted objectives. The actions done by the attacker are not limited to possible immediate effect on aeronautical safety, but rather, the limitations are determined by the aimed objectives. Cyber actions executed under detection levels ensure an unrevealed long presence in the adversary's systems, getting to know deeper the targeted systems and identifying the weak spots on the effect of cyber-attacks and implemented security measure, so that to ensure the success for the future cyber-attack, at the time and location desired by the cyber actor to be performed the attack. Plus, the attacker could have at its disposal and make use of it in a short time the latest equipment's or programs that are available for the public at large, as developed by private entities, The possibility to immediately use such goods is not handy for the one defending, because of the need to have interdependencies and effects of their use on the already existing components of the aeronautical system analyzed, process which requires a longer time than the one the attacker needs.

Even following a first analysis of cyber security for air forces, it becomes obvious that the advantage belongs to the one attacking, at least on the surface, the cyber defending measures are mostly reactive and not proactive. Therefore, it is important for the air forces to be able to minimize the effects of a cyber-attack, by raising resilience level of the cyber infrastructures.

Romania's Cyber Security Strategy defines[9] resilience of cyber infrastructures as being „*the ability cyber infrastructure components to withstand a cyber incident or attack and return to normality*".

It is of utmost importance that this return to normality of the air forces should be done within a time frame which ensures counterattacking the effects desired by the cyber actor through its cyber-attack, the impossibility to perform missions by the air forces' equipment and therefore causing the adversary to abort its action for whose support the cyber-attack has been used.

The 2007 Israeli Air Force Operation in Syria

The air bombing mission of 2007 executed by the Israeli Air Force is just one of the many examples which advocates for the need to adapt air forces to challenges of cyber space. Actions of the Israeli Air Forces in *Orchard operation* represented the completion of a process which began with the State of Israel obtaining information on the possibility that

[9] *Ibidem*, section 3, para. 16, accessed on 20.08.2020.

Syria might continue building nuclear facilities with the help of North Korean specialists. All information gathered in time have allowed the nuclear facilities to be identified within the proximity of the Euphrates river, later on being confirmed the nuclear destination of the facility by theft of information from an unprotected computer belonging to Syrian official. In addition to that were used special forces, which took samples of soil and water.

Syria tried to camouflage the military nature of its facilities, choosing not to place air defence assets next to the facilities; however, these attempts have only done nothing else but ease the attack. Once the analysis of available information was performed, the execution of the attack has been decided, by using aircrafts F-15 and F-16 from the Israeli Air Forces. There were suppositions on the way the Israeli aircraft managed to break through the Syrian air defence, among them being also the performance of a cyber-attack on Syrian air forces. Although information on the responsible for the attack were available, the State of Israel denied it, the confirmation being obtained far later, in 2018, when the bombing mission has been acknowledged.

Analyzing the mission from the point of view of the probable cyber-attack performed in support of the bombing mission, based on the information from available unclassified sources, there can be presented some conclusions on the need to adapt air forces to the challenges of cyber operations, both from the defense perspective, as well as the one of the cyber actor executing the attack.

Figure no. 1: Orchard operation[10]

From the defense perspective, the defensive forces were not able to implement cyber security measures necessary to counter-attack the effects of the cyber-attack. Moreover, the attack was not detected in due time, therefore contingency plans could not be applied and neither was the fightback to stop adversary's attack. Even if the Israel Air Forces have performed an air attack on Iraqi nuclear facilities in the year of 1981, locating the target deep in the territory and employment of air defense systems is likely to have led to the idea that it

[10] A. Harel, A. Benn, "No Longer a Secret: How Israel Destroyed Syria's Nuclear Reactor", *Haaretz*, 2018, URL: https://www.haaretz.com/world-news/MAGAZINE-no-longer-a-secret-how-israel-destroyed-syria-s-nuclear-reactor-1. 5914407, accessed on 23.08.2020.

is impossible to execute an air attack on a target which was camouflaged as to its special destination.

On the one hand, errors committed when evaluating the threat to the nuclear facilities determined building an insufficient defense, which did not include additional measures because of the need to hide the importance of the target. Furthermore, there have been under evaluated or not known adversary's possibilities in the cyber area. It is worth saying that it was only in 2010 when the virus Stuxnet has been discovered, the event could have warned the Syrian authorities about Israel cyber capabilities. As a consequence, even if on paper the Syrian armed forces present themselves as a strong force, the reality showed that, because they could not keep up with the new tendencies of military conflicts, all those impressive military capabilities were not able to discourage the enemy form executing its bombing mission, considering the risk of an armed counterattack of Syria.

On the other hand, the cyber actor performing the cyber-attack, could choose the exact timing to execute the cyber-attack, a moment determined on the basis of the operational needs of the bombing mission, confirming thus the advantage of attack over defense. Technological advancement, coming also from specific cooperation with the United States of America, has contributed to the success of the cyber-attack. The effects envisaged by the attacker, neutralizing the air defense of the adversary, show a deep knowledge of the systems and connections from within the Syrian air defense. Moreover, calibrating the actions within the cyber-attack has ensured the defense forces of the normality of the situation. Also, it is possible that the attack would not have gone above the minimum level to alert the Syrian forces. The probable cyber-attack was performed in support of air forces, evaluation of the importance attached to hitting the target by the Israeli authorities justifying its performance and exposure of its capabilities, under the risk that those capabilities to become operationally useless.

Conclusions

It is our opinion that, at the present moment, air power represents a potential determined by the acting capacities of modern air equipment which enclose top-level technology, but also to outdated air equipment, over which upgrading works have been done. All these should be able to execute specific mission in times of peace, crises or conflict. If for new aircrafts there has been attempt to implement cyber defense measures from the design phase, for other means implementing cyber defense is hard to do, because of high associated costs, low estimated exploitation duration of aircraft or because of technical difficulties of ensuring cyber defense.

In this context, cyber operations executed in support of actions performed with air forces have represented a triggering point and determined the international actors to take seriously the threats represented by cyber-attacks. Lack of training or impossibility to implement existing norms of cyber defense shall create the right framework for future successful cyber operations of the adversaries.

The apparent normality may hide serious deficiencies in cyber security, which are known by the adversaries and when they consider right, upon that moment, by performing a cyber operation, air power will be out of a possible conflict equation.

Integrating and synchronizing cyber operations with military operations offers transient and reversible solutions both for the disturbance of actions executed by the adversary's air power, and also for the increase of the effect of the operations performed by its own air forces. The secret nature of the information on offensive cyber activities is and will be a hindrance to achieve efficient adaptation to challenges of cyber operations.

In our view, the main characteristics of the contemporary air power, for an air power to operate in complex conflict environment should take into account the following:

- the apparent normality should not determine a relaxation of cyber security defense measures for an air force, ensuring cyber security must be regarded as a continuous process of maximum importance by continuing missions;

- by the evaluation of cyber threats for an air force or for an air component of joint military structure, there must be done an accurate, multidimensional and interdisciplinary analysis of the environment, which shall allow a correct and precise evaluation of the enemy's cyber threat level;

- integration of cyber security measure within air forces should be done in a shorter time, so as not to give way to the technological gap between the means of the attacker and those implemented in one's own air forces;

- resilience of the air forces should ensure the return to normality as before the cyber-attack, under the conditions of different cyber security levels for the used infrastructure. This condition assumes not only an adequate infrastructure and establishment of high level of national security, but also a culture of cyber security.

BIBLIOGRAPHY:

1. ***, *F.A.-1 – Doctrina pentru operații a Forțelor aeriene*, București, 2016 (In English: Air Forces Doctrine for operation), Bucharest, 2016.
2. ***, *System-of-systems notion of cybersecurity in aviation*, International Civil Aviation Organization, Thirteenth Air Navigation Conference, Canada, 2018, https://www.icao.int/Meetings/anconf13/Documents/WP/wp_270_en.pdf
3. ***, *F-117A Nighthawk Stealth Fighter*, URL: https://www.airforce-technology.com/projects/f117/
4. ***, *Cyber security strategy of Romania*, 2013, section 3, paragraph 2, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania
5. BEST, K.L.; SCHMID, J.; TIERNEY, S.; AWAN, J.; BEYENE, N.M.; HOLLIDAY, M.A.; KHAN, R.; LEE, K., *How to analyze the cyber threat from drones*, 2020, *RAND Corporation*, URL: https://www.rand.org/pubs/research_reports/RR2972.html
6. Harel, A.; Benn, A., *No Longer a Secret: How Israel Destroyed Syria's Nuclear Reactor*, 2018, URL: https://www.haaretz.com/world-news/MAGAZINE-no-longer-a-secret-how-israel-destroyed-syria-s-nuclear-reactor-1.5914407
7. SOF, E., *Operation Orchard: Bombing of the Syrian Nuclear reactor*, 2018, URL: https://special-ops.org/operation-orchard-bombing-of-the-syrian-nuclear-reactor/
8. WEINBERGER, S., *How Israel spoofed Syria's air defence system*, 2007, URL: https://www.wired.com/2007/10/how-israel-spoo/
9. R.M., *Israelul recunoaște, pentru prima oară, că a bombardat un „reactor nuclear" în Siria, în 2007/Avertismentul pentru Iran*, 2018, URL: https://www.hotnews.ro/stiri-international-22354250-israelul-recunoaste-pentru-prima-oara-bombardat-reactor-nuclear-siria-2007-avertismentul-pentru-iran.htm

CURRENT TRENDS IN MILITARY LOGISTICS MANAGEMENT

Cosmin-Florinel MITROI
Major, Ph.D. Student within "Carol I" National Defence University, Bucharest, Romania.
E-mail: mitroi13florin@yahoo.com

Abstract: *In the current security environment, the trend for national security logistics will be, in our opinion, a logistics focused on supporting the needs of the armed forces and will have the mission to provide the security system forces with the necessary civilian and military personnel, equipment, means of subsistence and essential support, at the requested destination, at the required time and in the requested quantity, during the operations designed to take place. The forces of the national military system will have to develop a logistics system in an integrated network of unitary action. The expected transformation will not take place immediately but will require essential changes, in stages, of the current logistics system, which will allow the forces of the national military system to train its personnel and modernize, but especially to be more rapidly deployable, highly maneuverable, sustainable and efficient.*

Keywords: *logistics; armed forces; military logistic trends; development; transformation.*

Introduction

Conflicts of a military nature (and not only them) which took place in the last part of the twentieth century and also the crisis situations and military actions of the early twenty-first century, showed that the problems of mankind were not solved with the disappearance of bipolarity, but on the contrary. The complexity of the politico-military phenomenon, its evolution and influence on society requires a careful, continuous and realistic analysis, in order to establish and develop policies, strategies, concepts and programs necessary to harmonize national efforts with those of international bodies and institutions, for modeling a new architecture of security and stability. In this context, the multi-dimensional character of the operating environment tends to become more integrated and almost completely focused on the cybernetic domain.

Military action, the beneficiary of prevision, planning, research and new initiatives, has undergone important changes, being characterized, at present, by complexity, mobility, dynamism and flexibility, and having as main pillar the use of high-performance capabilities of strike, of almost entirely professional forces, as well as integrated actions of services and / or types of weapons, in a complex environment in which they operate and against actors almost unknown in classical conflicts. From this perspective, the comprehensive approach to crisis situations implements a modern and efficient planning model, which considers the use, simultaneously or consecutively, of all the state instruments and means available he ground, air, naval, forces. In addition, benefiting from the new discoveries in the field of IT requires the immediate use of the Integrated Strategic Image (ISI) which requires a process of transformation of the Joint Task Force top-down so that forces are faster designed and rendered ready.

1. Military transformation – a requirement for the evolution of the security environment

New security challenges, generated by the overlapping of processes such as globalization and fragmentation, add to the classic forms of vulnerabilities, risks, and threats.

Asymmetric risks diversify and amplify in intensity and area of manifestation, and their prevention and countermeasure is a common responsibility of all states. Continuous conflicts, traditional outbursts of tension, phenomena of instability and crisis, trends of geopolitical redesign in some areas (Central Asia, Caucasus-Caspian Area, Middle East, Africa etc.) to marginalize or isolate some states, favors the existence and intensifying of risks and threats with a major impact on the national security of different states. In this context, there is an increase in the role of the international community and especially of international bodies specialized in resolving crises and stopping conflict situations in different parts of the world.

Without excluding war, perceived in the classical sense, future conflicts, specific to the industrial age, will be gradually replaced by those characteristics of the computer age. These will be predominantly asymmetric in nature, including actions against atypical forces. Military confrontations will be generally disproportionate in terms of technological potential, characterized by classic actions combined with intelligence warfare. The confrontations will be particularly violent in the initial phase and will have a different spatial-temporal scope, determined by the objectives planned at the outbreak of hostilities. The stabilization phase will substantially involve international civilian components.

Violence will manifest itself not only through combat actions but also through other forms and political, economic, media, psychological and informational means. The essence of the violence will be based on the use of new weapons and technologies, including those of mass destruction, as well as means that expand the confrontation in cyberspace.

The fundamental requirement of the transformation in this field is ,,the creation of an integrated logistics system with high mobility, which ensures the necessary logistics in the required place and volume, at the right time"[1]. The transformation in this field aims at operationalization, as well as hierarchical responsibility for the structures designed to generate and regenerate forces in the required volume and at the appropriate time. The sizing of these structures will be in relation to the specifics of the theater of operations and the mission to accomplish.

In the last 20 years, the Romanian military system has undergone an important conceptual and structural transformation, determined by constant changes in the security environment, but also by the access of our country to the NATO and EU structures. This transformation was needed in order to ensure the necessary capabilities to promote and defend national interests against current and future threats. At the national level, the primary goal of transformation is adapting the structure of the Romanian Army to the current and future security environment, to ensure the fulfillment of Romania's commitments as a NATO member. The process of reshaping the future military structure started, practically, in the early 1990's was practically started in the early 1990s, with the major political changes in Romanian society.

"During this period:

- the main laws and normative acts were adopted to ensure the optimal functioning of the military system, and for the next stage it is necessary to continue improving and adapting;

[1] ***, *Strategia de transformare a Armatei României*, Bucharest, 2007, available at www.mapn.ro › legislatie › documente › strategie_transformare_2007, accessed on 14 of July 2020.

- increased capacity for crisis management, prevention and counteracting threats to Romania's security;
- the system of transition of the army from the state of peace to the one of war was perfected."[2]

This transformation was necessary in order to „ensure the necessary capabilities to promote and defend national interests against current and future threats. We also needed this transformation in order to fulfill our commitments to NATO, the EU and other international security and defense organizations, which required both structural and organizational transformations, along with significant transformations in the structure of forces and related areas, such as capabilities, information, training and education, procurement, personnel management, budgeting and planning"[3].

The logistics of the services will be „complementary to the integrated logistics system. The necessary delimitations will be made between the mobile logistics command / execution structures, necessary for the deployable structures, the generation and regeneration logistics, with a double role (of mobile logistics and fixed logistics) and the fixed logistics necessary for the land, air and naval forces in peace, in crisis situations and in war."[4] The capacities of procurement, storage, patrimony management and capitalization will be developed.

2. The evolution of logistics management – current trends

Throughout history, it has been shown that technical progress in equipping armies has always had a strong impact on troop logistics, often decisively influencing the way in which logistical support was provided. We do not intend to resort to history, but we believe that it is enough to recall the impact that the introduction of helicopters had on the transport and supply of troops in conflicts that took place after the Second World War. We appreciate that it is likely that the future of the logistics environment will be influenced by technical advances made in the following six areas:

- improving the collection of information through the use of electronic aerial surveillance sensors;
- development of new types of intelligent ammunition, of high precision, which will allow the execution of "punctual" hits;
- increasing the role of anti-aircraft defense for the protection of communication lines and the sites where logistics units, subunits and formations are deployed;
- improving communications at the tactical level by using satellite communications and mobile technology, which will increase the accuracy of information on the operational situation and the possibility of making the decision to transmit orders in real time;
- improving the possibilities to execute deep operations both by using aviation and ground attack capabilities, knowing that, in the conditions of modern warfare, a possible aggressor will primarily seek to disrupt supply lines and disorganize the logistics system.

Efforts are currently being made to increase the effectiveness and efficiency of logistics by planning resources according to the principle of total management, by integrating logistics activities into military operations and by increasing the speed of logistical response

[2] Florian Râpan, *Coordonate ale modernizării managementului resurselor de apărare*, available at http://www.codrm.eu/conferences/2007/09_RAPAN_FLORIAN.pdf, accessed on 15 of July 2020.
[3] Virgil Ristea, *Armed forces transformation to counteract the security environment challenges*, January 2019, available at https://www.researchgate.net/publication/242476514_ARMED_FORCES_TRANSFORMATION_TO_COUNTERACT_THE_SECURITY_ENVIRONMENT_CHALLENGES, accessed on 21 July 2020.
[4] Gheorghe Minculete, *Abordări moderne ale managementului logistic*, "Carol I" National Defence University Publishing House, Bucharest, 2015, pp. 110-111.

to the use of network forces. This requires qualitative changes in military logistics for: „the integration of suppliers, consumers and resources in a subsystem integrated into the network system; real-time logistics management and control; action continuity and prevention of blockages; integration of all logistical bases in the logistical support of theaters of operations, of each action element of theaters of operations; shifting efforts from optimizing logistics efficiency to optimizing network system efficiency; ensuring integrated, dynamic and continuous logistical support; integration of logistical functions with informational ones within the substantiation of decision making etc."[5]. Only in this way can logistics be transformed „from a form of securing forces into one of multiplying forces in order to contribute to increasing military effectiveness and achieving success".[6]

Based on the requirements and priority directions established in the „Romanian Armed Forces Transformation Strategy", the logistics system of the force structure in the Romanian Armed Forces is currently undergoing the most extensive reconfiguration process in the last ten years. The transformations aimed at invigorating logistics both as a whole and in its functional areas, by implementing new concepts and creating functional organizational structures, necessary for alignment and integration in NATO logistics. These transformations are characterized as follows:

- **conceptually**: redefining essential concepts at general and particular level, such as: integrated logistics system; logistical support; management and execution of the logistics system on hierarchical levels, having as main pillar the logistics base; production, consumption and multinational logistics; integration of the functional domains of logistics;
- **structurally**: the emergence of new types of units – logistical bases for all services and branches commands, operational support units, logistical support units, maintenance sections for military equipment, specialized warehouses;
- **functionally**: redefining the missions and responsibilities of the logistical support units; harmonization of logistics flows in relation to financial flow; concentration and management of resources to / from the logistics bases.

The demands in the field of logistics require the creation of a mobility support system, able to provide support where it is needed, in the required volume and at the right time. From our point of view, we consider it is necessary, first of all, to be able to determine the requirements of logistics and those associated with it in a coherent way, because the successful implementation of the principles of logistical support, as well as the concepts – this field is certainly a necessity for the efficient understanding of the whole current operating environment. In this sense, it is considered that „...there is a number of directions that seem to be significant, common, although individual perceptions differ depending on personal observations and experiences".[7]

We can emphasize that, in the near future, the need for flexibility of logistics structures will generate new initiatives in relation to the conquests for which they were designed and those to support the fighting forces. Once established, the large units, units and subunits for logistical support „will have to adopt not only a new, predictive and proactive way of ensuring logistical support for the fighting forces".[8]

---

[5] Michael S. Ewer, *An analysis of department of defense policy and guidance for implementation of performance-based logistics, Master Thesis of Science in Systems Engineering Management from the Naval Postgraduate School Monterey*, California, September 2015.

[6] Michael Huggos, *Essentials of supply chain management*, 2003, ISBN 0-471-23517-2, p. 258.

[7] Lăpădat Dan, *Logistica de producţie şi consum a sistemelor de apărare*,localitate, Research Agency for Military Technology and Technologies, Bucharest, 2008, p. 6.

[8] ***, *Romanian Armed Forces Transformation Strategy*, Bucharest, 2009, available at www.mapn.ro › legislatie › documente › strategie_transformare_2009, accessed on 15.06.2020.

Based on the characteristics and defining elements of the current logistics system, the general and specific requirements of the logistics system transformation and modalities of action can lead to accelerate the process of transforming the logistics system.

The general requirements of the transformation include: the establishment of management structures, with responsibilities in the planning, management and control of activities in the field of logistics and execution logistics structures; configuration of viable logistics structures, which ensure the optimization of the functional domains of the logistics system; ensuring operational, flexible logistical structures, in accordance with the hierarchical level, nature, value and missions of the force for which the logistical support is provided; removing parallels and overlaps regarding the development of acquisition system of materials and supply for services; reducing the reaction time in carrying out activities in logistics and developing the anticipatory nature of logistics; covering the underdeveloped order of activity of the current systems – outsourcing services and maintenance, reducing surplus materials and capitalizing on them, coding and standardization in the logistics field, training and specialization of logistics staff; making and maintaining stocks of material goods according to the concept of stocks.

We appreciate that, in order to ensure the necessary balance between desire and resources, it is necessary to take into account, in general, the economic performance of Romanian society at present, „...and in particular, the characteristics of the military system, the resources made available to the military body by the political factor, which, in the end, provides the necessary information about the effectiveness and efficiency of the logistics system."[9]

In order for the armed forces to be prepared today to participate in the war of the future, it is necessary to solve the following problems: „transforming the supply-distribution chain into a networked supply system simultaneously with changing supply methods; supporting expeditionary forces through flexible logistical bases that can operatively move and act modularly; reducing the risk of negative influences of military operations by eliminating supply gaps right from the planning period; awareness regarding the needs for logistical support from peacetime; integration of all resources into an overall system, able to support all forces operating in theaters of operations etc.".[10]

Conclusion

The current logistic system of the forces pertaining to the national defense system is of reactive type, assuming a request, when a need is necessary and therefore requested, identifying the procedures for fulfilling this need and satisfying it, which leads to a high consumption of time, with negative repercussions in terms of the pace of conducting a military operation. This system has often led to serious disruptions in providing timely logistical support for the fighting forces and, consequently, must be transformed from reactive to pro-active, based on a new vision, higher flexibility and better anticipation.

A proactive system requires realistic estimate of the logistic support needs and their satisfaction by prepositioning the logistic support where the need for support must be met and implicitly the shortening of the necessary logistic time. So, we believe that, in order to achieve these transformations, it is necessary to create a new environment in which logistics is

[9] Mocanu, Bixi-Pompiliu, *Considerations regarding the evolution of the concept of logistics - Current trends*, Regional stability and security, Scientific Communications Session with International Participation, "Carol I" National Defence University, Bucharest, 2009.
[10] ***, *Pagini din gândirea militară universală*, volumul II, The Military Publishing House, Bucharest, 1985, p. 259.

proactive and not reactive, in which capability requirements are anticipated and not developed as a result of needs materialized by request.

These transformations closely followed the evolution of logistics and aimed to achieve the highest possible level of availability of military technical systems, in conditions of economic efficiency. The transition to modern logistics systems through changes in concepts, policies and principles has led to reconsidering the importance of monitoring the operating parameters of the supply-distribution system within logistics management.

Currently, the evolution of the concept is identified by making innovative combinations of logistics principles in an adaptive, collaborative way, by using all logistics skills, based on the use of potential partners, allies or their own possibilities.

The future will not necessarily be on the side of those technologically advanced, but especially on the part of those forces capable of reacting quickly to major changes and adapting quickly and efficiently to those requirements imposed by the constantly changing nature of the security environment.

BIBLIOGRAPHY:

1. ADAMS, I., *Managementul organizaţiei*, Economic Publishing House, Bucharest, 2008.
2. ALNIŢEI, Marin, "Imaginea recunoscută a mediului Joint şi Imaginea Strategică Integrată în războiul viitorului", in *Gândirea militară românească*, no. 6 from 2010, The Tehnic Military Center Publishing House, Bucharest, 2010.
3. BĂDĂLAN, Eugen; UDRESCU, Mircea; MINCU, Constantin, *Condiţionări logistice în epoca globalizării*, Academy of Romanian Scientists Publishing House, Bucharest, 2010.
4. RĂPAN, Florian, *Coordonate ale modernizării managementului resurselor de apărare*, URL: http://www.codrm.eu/conferences/2007/09_rapan_florian.pdf
5. HUGGOS, Michael, *Essentials of supply chain management*, 2003.
6. KORTSHAC, Bernard Helmut, *Ce este logistica?* Logistic Systems Publication, no. 2, Bucharest, 1991.
7. MINCULETE, Gheorghe, *Abordări modern ale managementului logistic*, "Carol I" National Defence University Publishing House, Bucharest, 2015.
8. MINCULETE Gheorghe, UDRESCU Mircea, ANDRONIC Benone, *Elemente de logistică economică*, "Carol I" National Defence University Publishing House, Bucharest, 2010.
9. SITEANU, Eugen, *Logistica de producţie*, The Technic Military Academy Publishing House, Bucharest, 2009.
10. SITEANU Eugen, *Management general*, Ion I. C. Brătianu Academy Publishing House, Bucharest, 2001
11. ZORLENŢAN T., BURDUŞ E., *Managementul organizaţiei*, Economic Publishing House, Bucharest, 1998.
12. LĂPĂDAT Dan, *Logistics for production and consumption of defense systems. Study on the concepts of logistics on the life cycle of systems*, Research Agency for Military Technique and Technologies, Bucharest, 2008.
13. MOCANU, Bixi-Pompiliu, *Considerations regarding the evolution of the concept of logistics*, Scientific Communications Session with International Participation, „Carol I" National Defense University, Bucharest, 2009.
14. ***, *S.M.Ap. 57/2020, The Doctrine of the Joint Logistics of the Romanian Army*, Bucharest, 2020.

THE SECURITY IMPLICATIONS OF CRYPTOCURRENCIES

Maria CONSTANTINESCU, PhD.
Associate Professor, DRESMARA, Brasov, Romania. E-mail: mconst_ro@yahoo.com

Abstract*: Cryptocurrencies were initially regarded as a technological curiosity and a way to put into practice the principles of the libertarian ideology. A decade later from the emergence of the first cryptocurrency, they have slowly made their way in many aspects of the real world and have been widely embraced, for legitimate or illicit purposes. Consequently, cryptocurrencies now have a variety of security implications, at national and even global scale. These implications derive first of all from their use for illegal activities (from terrorism to money laundering and financing the activities of organized crime networks), but also from their legal use, through their influence on the financial sector, on a country's monetary policy or through private initiatives such as the Libra project initiated by Facebook. The purpose of this paper is to analyse these security implications and the measures that states can take to mitigate their negative impact.*

Keywords*: cryptocurrencies; security implications; terrorism; organized crime; monetary policy.*

Introduction

The concept of *cryptocurrencies* and the blockchain technology that underlines them are a fashionable phenomenon, but one surrounded by misconceptions, prejudice, and myths. One of the most popular cryptocurrency is Bitcoin, hailed by some of its supporters as an alternative to the fiat money (issued by nation states) or as a profitable investment tool, while its detractors emphasize its volatility, speculative nature and the its potential use for illicit activities.

Bitcoin was developed by its mysterious creator (creators) known as Satoshi Nakamoto as "a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution"[1]. From its inception, Bitcoin (and by extension all the other cryptocurrencies) were aligned with the libertarian ideology, which advocates the minimization or even elimination of the state's authority on the society. According to this ideology, the state exerts an excessive control over the society, through many means, among which the control of information and personal data[2]. From the point of view of ensuring the national security, the libertarian ideology in itself can be considered a security risk, and many of its supporters are involved into anarchist or extremist movements.

Although cryptocurrencies do have a dark side, they should not be reduced only to the negative aspects that make them a potential risk for national security. The purpose of this paper is to analyse these security implications and the measures that states can take to mitigate their negative impact. But we have to keep in mind that cryptocurrencies, and especially the

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, accessed on July 07, 2020.
[2] David Boaz, *The fundamentals of the theory of liberty*, Libertarianism.org, 2019, URL: https://www.libertarianism.org/essays/what-is-libertarianism, accessed on July 19, 2020.

blockchain technology they are based on, also have a number of interesting features that could be used to produce positive effects.

1. Defining cryptocurrencies

In order to identify the security implications of cryptocurrencies, we have first to define them, which is not an easy task, as there is no universally accepted definition and the concept can be analysed from various points of view: technical, economical or even ideological.

First of all, we have to make the distinction between a digital currency and a virtual currency[3]. A *digital currency* is a currency that exists only in digital format, it does not have a physical form (such as cash in banknotes or coins), which means that it can only transferred, stored and spend in the digital environment, in inter-connected networks. Fiat money (the national currencies, such as lei, dollars or euro) can have a digital form (in the accounts of a bank), but they can also be transformed into physical money, for example when we take money from an ATM.

A virtual currency is a type of digital currency, but the concepts are not synonymous, as not any digital currency is simultaneously a virtual currency. According to the definition of the Central European Bank, a *virtual currency* is "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"[4]. The European Banking Authority defines a virtual currency as "a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a Fiat Currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically"[5].

An important difference between the digital currency and the virtual currency is that the latter is not issued by a centralized authority and its value is not based on a real economy (as it is the case with the digital form of the fiat money). Virtual currencies circulate within a specific virtual community and their value is based on the criteria decided by that particular community. A well-known example is the Linden dollar that exists only in the users of the Second Life 3D virtual world (a computer game).

Coming back to the definition of cryptocurrencies, they may be defined as "a digital currency in which encryption techniques are used to control the generation of units of currency and verify the transfer of funds, operating independently of a central bank" [6]. Another definition refers to cryptocurrencies as "digital medium of exchange using strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets[7]".

To sum up, a cryptocurrency is a type of virtual currency that uses IT and economic principles and cryptography to ensure the security of the information regarding the transactions. A main characteristic of the cryptocurrencies, that makes them attractive, is the fact that they are decentralized (are not issued by a central authority) and use complicated encryption techniques. In theory, this makes them immune to external control and influences

[3] URL: https://www.investopedia.com/terms/d/digital-currency.asp, accessed on July 14, 2020.
[4] *Virtual Currency Schemes*, Central European Bank, 2012, p. 13, URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, accessed on June 02, 2020.
[5] *EBA Opinion on 'virtual currencies'*, European Banking Authority, p. 11, URL: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, accessed on July 10, 2020.
[6] Patrick Schueffel, *The Concise Fintech Compendium*, p. 9, Fribourg: School of Management, 2017, Fribourg, Switzerland, URL: http://schueffel.biz/wp-content/uploads/2017/09/Schueffel-2017-The-Concise-FINTECH-COMPENDIUM.pdf,, accessed on July 10, 2020.
[7] URL: https://coinmarketcap.com/intro-to-crypto/what-are-cryptocurrencies, accessed on July 18, 2020.

and ensures a high degree of privacy and confidentiality without the need to rely on a trusted third party. Another difference between cryptocurrencies and fiat money, which makes them attractive, but also a security risk, is that while the transfer of funds in fiat money through official channels usually requires identification, cryptocurrencies ensure the anonymity of the users. In the crypto community the rules are set an enforced by the members of the community, not by state authorities, and transactions are more difficult (but not impossible) to trace than those taking place through banks or other financial institutions.

Cryptocurrencies appeared based on the belief that the creation, distribution, use, and control of money should not be the monopoly of a state or central bank, through policies and regulations. As cryptocurrencies (and especially Bitcoin) have made their way in the mainstream, they have become attractive to a larger category of users than the initial IT enthusiasts and adepts of the libertarian ideology. Their appeal extended to a wide variety of users, from members of the organized crime and terrorist groups to financial speculators, from regular individuals attracted by a new buzz-word to state actors wishing to evade economic sanctions.

2. Security implications of cryptocurrencies

Cryptocurrencies have emerged as a technological and financial revolution, but they can also generate multiple security threats, from their use by terrorist organizations or organized crime structures to promoting speculations and the use of financial instruments that may increase the instability of the financial markets. Long-time considered as yet another technological fad that will disappear by itself, they have only recently began to be recognized as an emerging security threat: "one of the greatest emerging threats to U.S. national security is illicit use of virtual or cryptocurrencies" [8].

2.1. Cryptocurrencies as tools for money laundering and organized crime activities

One of the main threats to national security comes from the use of cryptocurrencies as a tool for money laundering and for financing various organized crimes activities.

Due to their decentralized nature and high degree of anonymity, cryptocurrencies have become attractive as a tool for money laundering, especially after the emergence of the decentralized exchanges (internet sites that provide exchange services from cryptocurrencies to hard currency). The (still) loose regulations in this area allow illegal funds to be transformed with a high degree of privacy, as long as these exchanges remain outside the regulatory framework that govern the other financial institutions, that have to comply with the Anti-Money Laundering (AML) and Know Your Customer (KYC) laws and regulations. According to a study by Coinfirm, from the 216 exchanges studied online, 69% do not have complete and transparent" KYC procedures and only 26% of exchanges had a "high" level of AML procedures, such as ongoing transaction monitoring and in-house compliance staff with experience in AML[9].

Cryptocurrencies emerge as a key mean for payment for illegal services, procurement of illegal goods on Darknet markets, of payments resulting from ransomware, Distributed Denial of Service or other organized crime methods. In this respect, Bitcoin remains the most

[8] Andrew Munro, *Privacy cryptocurrency among "greatest national security threats" Secret Service says*, URL: https://www.finder.com.au/privacy-cryptocurrency-among-greatest-national-security-threats-secret-service-says, accessed on July 05, 2020.

[9] Leigh Cuen, *Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report*, 2019, URL: https://www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report, accessed on July 15, 2020.

popular cryptocurrency used in cybercrime within the EU, even if its market-share is declining in favour of private cryptocurrencies (such as Monero or Zcahs)[10]. This trend derives from Bitcoin's pseudo-anonymity, as its level of privacy is not as high as the illicit users might like. Transactions in Bitcoin can be traced (although it is not an easy feat) through tracing the history of the transactions, the IP address and other means that would link transactions to a digital wallet. The way the FBI managed to dismantle Silk Road, which was at that time the biggest drug traffic network on Darknet, by tracing Bitcoin transactions to the owner of the network, is a case in point.

Cryptocurrencies are also linked to another type of cyberattack, ransomware (through various means, such as spear phishing, malware or SIM swapping). The ransomware activity is a rising trend and a very lucrative illegal business, amounting just in the US in 2019 to 75 billion dollars[11]. Cryptocurrencies are ideal as a tool for the hacker to safely get the ransom money, as they provide a high degree of anonymity and are a lot more difficult to trace than cash or bank transfers.

Cybercriminals that desire a low profile can also use crypto-jacking attacks performed through "the unauthorized use of someone else's computer to mine cryptocurrency... by either getting the victim to click on a malicious link in an email that loads crypto-mining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser"[12].

Cryptocurrencies can also be used for depositing funds resulting from illegal activities, far from the eyes of the regulatory authorities. For example, in May 2018, the Spanish, Bulgarian police and the Europol have dismantled a criminal network involved in money laundering, burglaries and drug trafficking, and through the assets seized were 220.000 euro in cryptocurrencies[13].

2.2. Cryptocurrencies as tools for financing terrorist activities

The increasing use of cryptocurrencies by organized crime networks leads to the obvious question of their use by terrorist organizations. Although there are cases when cryptocurrencies have been used to gather financial support for terrorist activities, until now the amounts of funds have been relatively small, but this trend can change in the future.

Terrorist organizations may find cryptocurrencies appealing for the same reasons they are attractive to organized crime networks, the high degree of anonymity for users and transactions, their global nature that makes possible the transfer of funds internationally with relative ease and the difficulty to trace the provenance/destination of the funds by law enforcement or other state authorities.

Many governments have increased in the last 20 years their efforts to trace funds transfers, as a tool for counter-terrorism activities, which lead to the adoption by terrorist groups of alternative means of funds transfer, such as pre-payed debit cards or alternative online payment systems (such as PayPal, AmazonPay, Google Wallet). Cryptocurrencies have the potential to be adopted as an alternative mean of gathering and transferring funds to

---

[10] *Internet organized crime threat assessment*, Europol, p. 54, 2019, URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, accessed on July 22, 2020.

[11] *Idem.*

[12] Michael Nadeau, *What is cryptojacking? How to prevent, detect, and recover from it*, 2020, https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html, accessed on July 26, 2020.

[13] *Poly-criminal group involved in money laundering, home burglaries and drug trafficking busted*, Europol, 2018, URL: https://www.europol.europa.eu/newsroom/news/poly-criminal-group-involved-in-money-laundering-home-burglaries-and-drug-trafficking-busted, accessed on July 05, 2020.

support terrorist activities. For example, Islamic terrorists based in Middle East countries used a combination of methods, namely Bitcoin and PayPal, to fund their terrorist activities in Indonesia as these type of transactions are harder to trace[14]. The DarkNet is a friendly environment in which there have been some attempts to raise funds in bitcoin for terrorist activities (namely for ISIS)[15].

Still, there are also significant differences between organized crime activities and terrorist activities, which makes the latter less eager to embrace cryptocurrencies. Unlike organized crime networks, so far terrorist organizations have not adopted cryptocurrencies on a large scale, for reasons specific to their activities. In using of this type of currencies to finance their activities, terrorist groups would be as vulnerable as normal users to the high volatility of the cryptocurrencies prices, which makes them less trustworthy as fiat money. Also, cryptocurrencies are a lot more vulnerable to cyber-attacks that fiat money, which makes them harder to use by inexperienced individuals.

Many terrorist groups act in areas where electronic banking, or even internet access, is not as easily available as in more stable/developed countries, which makes them prone to use more traditional methods of financing and money transfer that have already proven their effectiveness. A Financial Action Task Force report considers that informal, cash based, economies of many Central and West African countries, with porous borders and almost complete lack of financial supervision, create opportunities for anonymous cash transfers which make electronic transfers less useful[16].

Also, the lack of access to digital infrastructure is compounded in many countries where terrorist organizations act, by the level of technical abilities and computer literacy required to use cryptocurrencies. Terrorist organizations such as Boko Haram, ISIS, AQIM, and others operate in hostile and less developed areas, where the literacy level is low and have no practical reasons to complicate their life and activity by embracing financing through cryptocurrencies. It would be useless for them to have 1,000 Bitcoin if they can't exchange them for dollars in order to buy weapons, food, supplies or to bribe local authorities.

Terrorist organizations already use trusted and tried methods of financing, such as hawala or transfers through banks run by sympathisers, and they don't have too many reasons to change them. For example, ISIS obtained significant funds from taking over resource-rich locations (for instance oil fields and refineries) through extortion, kidnappings, lootings and they have little incentive to turn to such complicated ways of getting financing as cryptocurrencies. Hezbollah relies on financial support from other states, which eliminates the need to use cryptocurrencies, as they can get funds easily and safely through legal transfers by using banks owned by supporters of their cause.

Terrorist groups may be tempted to use cryptocurrencies when part of their financing relies on sources related to organized crimes activities (such as drug traffic), as they are more extensively used by the latter as we have mentioned above.

---

[14] Resty Woro Yuniar, *Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says*, The Wall Street Journal, 2017, http://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198, accessed on July 11, 2020.

[15] Danna Harman, *U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*, Haaretz, 2015, http://www.haaretz.com/middle-east-news/.premium-1.639542, accessed on July 11, 2020.
Adam Taylor, *The Islamic State (or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin*, The Washington Post, 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamicstate-or-someone-pretending-to-be-it-is-trying-to-raisefunds-using-bitcoin/?utm_term=.17ae7b7b7221, accessed on July 11, 2020.

[16] *Money Laundering Through the Physical Transportation of Cash*, Financial Action Task Force, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf, accessed on July 14, 2020.

2.3. Cryptocurrencies as tools for tax evasion

Cryptocurrencies are also used in combination with alternative means of payments in order to avoid taxes or the regulations imposed by states for money transfers. For instance, the Chinese businessmen activating in Russia use the cryptocurrency Tether to transfer large amounts of money to China, to circumvent strict capital transfer rules[17]. The market generating these transfers is significant, according to the estimation of the Russian Central Bank the retail black market in Moscow was in 2019 around 9.4 billion USD, with a large part of these gains transferred to China in the form of cryptocurrencies[18].

Fiscal authorities in many countries attempt to enforce regulations that tax crypto-to-crypto transactions and crypto-to-cash transactions, from the moment they are registered in an exchange, but this still doesn't mean that cryptocurrencies cannot be used successfully for tax evasion. Cryptocurrencies owners can donate money to non-profit organizations, in total anonymity and without the need to justify the provenience of the funds, or they can use the services of crypto lenders and place cryptocurrencies under their custody, using it as collateral to buy even more cryptocurrency or borrow cash. Deriving from the anonymity of the transactions, the fact that a cryptocurrency electronic wallet is not linked to the real world identity of its owner, cryptocurrency owners can easily escape the vigilance of the fiscal authorities. The only moment when their funds become more visible for taxation is when using the services of an exchange, but the regulatory framework of exchanges is not harmonized internationally and there are still numerous exchanges functioning illegally, which cannot be controlled.

The global nature of cryptocurrencies makes them the digital equivalent of tax heavens, and a useful tool for hiding the provenance of funds. In terms of national security, this generates additional difficulties in countering organized crime, foreign interventions and influences, terrorist activities, etc.

3. Political, economic and informational implications of cryptocurrencies

The security implications of cryptocurrencies mentioned above share similarities with the implications of illegal activities such as drug trafficking and other forms of organized crime. Due to their characteristics, cryptocurrencies may have wider implications on security, in the areas of politics, economics and information.

3.1. The use of cryptocurrencies by state actors

In the context of the hybrid warfare, state actors have not ignored the potential uses of cryptocurrencies. One of the characteristics of the information war waged online is the difficulty of proving the links between trolls, fake news sites or individuals and the states that use these means to achieve strategic goals. The states involved in these activities can at any time claim that the trolls or sites were acting in their personal name or even that they were coordinated in the shadows by other states. Cryptocurrencies may play a role in this type of war in several ways.

Cryptocurrencies may be used to fund espionage and information warfare activities, but also for obtaining capital gains. Special Prosecutor Robert Mueller's report states that

[17] Anna Baydakova, *Millions in Crypto Is Crossing the Russia-China Border Daily, Tether Is King*, 2019, URL: https://www.coindesk.com/tether-usdt-russia-china-importers, accessed on July 04, 2020.

[18] *The Central Bank estimated the shadow turnover of the Moscow markets at 600 billion rubles*, https://www.rbc.ru/finances/12/04/2018/5acf26f59a79471ae61bfbc9https://www.rbc.ru/finances/12/04/2018/5acf26f59a79471ae61bfbc9, accessed on July 14, 2020.

Russian intelligence services have used Bitcoin to fund their operations[19]. According to the report, Russian agents used cryptocurrencies in many stages of the operation. Bitcoin was used to acquire the systems used to hack the emails of Democratic Party members and to pay the online hosting services on the platforms that published the materials thus obtained. The report shows that Russian agents intended to use the anonymity of cryptocurrencies to their advantage in order to hide their real identities and the source of funds.

Informational warfare campaigns can be combined with cryptojacking activities as any additional source of financing is welcome. An example is the site *infopolk.ru*, which was guiding its users to a series of pro-Russian sites and had a series of add-ons that allowed the user to spread that content on social media. In addition to the pro-Russian propaganda, that particular site was also running a cryptojacking code, which was hijacking the user's computer power to mine cryptocurrencies[20]. It is difficult to establish without a thorough investigation whether the site actually had links to Russian intelligence services, was run by materialist "patriots" trying to combine ideology with profit, or was simply a purely profit-oriented site that attracted naive pro-Russians users in order to make a profit. In any case, the example is illustrative of the various ways in which a state could even obtain funding for propaganda activities and at the same time conducts propaganda activities.

Cryptocurrencies can be used by state actors to promote extremist ideology, as the risks to national security may come from other states that support and finance specific groups promoting extremist ideologies. Far-right groups have shown a particular interest in using cryptocurrencies, as their ideology has common features with the libertarian ideology. David Columbia[21] examines the history of some of the extremist ideas that founded Bitcoin, such as be the international conspiracy of Jewish bankers, and how these ideas were propagated in the Bitcoin ecosystem even if most current cryptocurrency supporters reject the origin of these ideas. The author concludes that the percentage of extremists in the crypto ecosystem is higher than in the general population, even if in real terms, the number of fascists or Nazis among cryptocurrency users is small. According to Columbia, this is due to the specific culture embraced by those who use cryptocurrencies for ideological reasons, who are generally more willing to believe in conspiracy theories and have an attitude of rejection of the "real" society, perceived as corrupt[22].

Another area where cryptocurrencies have been used by state actors are related to the mitigation of the effects of the economic sanctions. For instance, IBENA, Iran's only economic news network, had announced in 2018 details regarding a potential cryptocurrency issued by the Iranian state[23] to facilitate money transfers to and from other countries and diminish the influence of the SWIFT payment system controlled by the US, in order to mitigate the effects of the economic sanctions.

Venezuela is the first country that attempted to implement cryptocurrencies on a large scale in order to avoid US economic sanctions and boost its economy devastated by hyperinflation. Thus, in 2018, Venezuela issued 100 million Petro (its cryptocurrency), whose price is indexed to the price of a barrel of oil[24]. The cryptocurrency was heavily promoted

[19] Robert Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Washington, D.C. March 2019, https://www.justice.gov/storage/report.pdf, accessed on July 19, 2020.
[20] URL: https://medium.com/dfrlab/russian-info-war-pages-removed-a894b2dc34f0, accessed on July 19, 2020.
[21] David Columbia, *The Politics of Bitcoin: Software as Right-Wing Extremism. of Bitcoin: Software as Right-Wing Extremism*, Quinn DuPont, 2017.
[22] *Idem*.
[23] *Iranian Cryptocurrency's Features Revealed*, http://en.ibena.ir/news/90482/Iranian-Cryptocurrency-s-Features-Revealed, accessed on July 19, 2020.
[24] John Buck, *President Maduro: Venezuela to Issue First 100 Million Petros*, 2018, https://coin telegraph.com/news/president-maduro-venezuela-to-issue-first-100-million-petros, accessed on July 25, 2020.

domestically, with Maduro announcing that Petro would be used as a unit of account by state oil company PDVSA[25] and the government aimed to introduce a new wage and pricing system for this cryptocurrency. Petro is traded in state-authorized exchanges and basically starting from 2018 Venezuela officially has two national currencies, Petro and the sovereign bolivar, the latter being indexed to the cryptocurrency. As a measure to motivate the population to use Petro, the government offered a 10% reduction in the payment of taxes and other contributions to the state budget with this cryptocurrency.

Another way in which cryptocurrencies can have negative influences on the national security derives from the fact that they can be used by state actors to influence the result of elections in another country. For example, in the US, the Centre for Public Integrity has found that in the 2018 legislative elections there were 20 crypto-candidates from across the political spectrum, who ran for all levels of representation and who requested and/or received cryptocurrencies to fund their campaigns[26]. At least three of these candidates came from states that have since banned such donations and another has accepted cryptocurrencies that cannot be traced.

Politicians around the world could not be elected without an election campaign, which means solving the thorny issue of funding. There are honest politicians who reveal the sources of funding, but also politicians who have an interest in hiding the amounts of money received from various lobbies or interest groups whose support would not be to the liking of the electorate. Imagine an environmental candidate who is found to have been financed by an oil group or an active defender of national sovereignty who is proven to have been financed by a rival country. The prospect of political candidates being financed through virtually untraceable funds by other states can pose serious risks to a country's national security, as the candidate, once in power, will act in accordance with the interests of the financier, and cryptocurrencies make it possible to hide the origin of funds from the public and the authorities of the electoral process.

3.2. The impact of cryptocurrencies mining on energy security

Cryptocurrencies mining is an energy-intensive process requiring a large electricity consumption. According to Digiconomist, in 2018 the energy consumption required for Bitcoin mining amounted to 70% of the entire annual electricity consumption of the Czech Republic[27]. As a result, cryptocurrency mining, especially when done on a large scale in mining pools, can have serious negative impacts on a country's energy security.

For example, China is one of the countries that hosts most of the mining pools (according to bitcoin.com, 65% of global Bitcoin hash rate is concentrated in China)[28], thanks to cheap electricity in the Xinjiang and central Mongolia coal fields, as well as cheap hydro-electricity in the rainy season in Yunnan and Sichuan provinces. This intensive activity, however, has a cost, considered too high by the Chinese authorities. They envisage limiting or even banning cryptocurrencies mining on the territory of the country, because it considers that the activity consumes too much energy and is polluting the environment. Thus, the main planning authority of the Chinese economy, the National Development and Reform Commission, has published a list of industrial activities that the Chinese state wants to

[25] https://www.abc.es/internacional/abci-maduro-anuncia-petrolera-pdvsa-usara-criptomoneda-petro-como-unidad-contable-201808140459_noticia.html, accessed on July 25, 2020.
[26] Kristian Hernandez, *How cryptocurrency is sneaking into state elections*, Politico Magazine, 2018, https://publicintegrity.org/politics/state-politics/how-cryptocurrency-is-sneaking-into-state-elections/ accessed on July 25, 2020.
[27] https://digiconomist.net/bitcoin-energy-consumption, accessed on July 25, 2020.
[28] Jeffrey Gogo, *65% of Global Bitcoin Hashrate Concentrated in China*, https://news.bitcoin.com/65-of-global-bitcoin-hashrate-concentrated-in-china, accessed on 02 August 2020.

restrict[29], as they would be incompatible with the legislation in force, insufficiently safe, too polluting or wasting resources. The cryptocurrencies mining is in the category of activities to be completely prohibited.

Even though the cryptocurrency sector is lucrative, the measure reflects the "industrial policy of the country"[30], which gives priority to production activities. China needs huge amounts of resources (including electricity) to support the production-based economy, so that the cryptocurrency mining sector competes directly with commodity-producing enterprises for access to scarce energy resources.

3.3. The impact of cryptocurrencies on financial stability and monetary policy

From the point of view of financial and economic security, cryptocurrencies may have a potential negative impact due to their high price volatility, deeply speculative nature that generates high risks for potential investors but can also destabilize the financial system.

The recent Facebook attempt to launch its own cryptocurrency, Libra, has brought to the attention the potential risks to the stability of a country's financial and economic system generated by a profit-driven, large corporation aiming to put into practice the libertarian ideology of eliminating the state's role in society and economy.

The idea of corporations launching their own cryptocurrencies, which would run in parallel with the official national currency, is extremely dangerous as it would prevent the use of the monetary policy tools at the disposal of the central bank to regulate the economic activity. It would also affect negatively the functioning of the financial and banking system, which have already proven how dangerous they are when not properly regulated in the 2008 financial crisis. A cryptocurrency issued by a private company with global reach would be even more difficult to regulate than the traditional banking and financial institutions, with serious implications on the national security.

Conclusions

Cryptocurrencies were created as an alternative to the classic banking and financial system, but their relative success with investment firms, private companies, and ordinary citizens indicates that they have become connected to the real economy. This means that the governments can no longer afford to ignore the phenomenon and in particular its implications on the national security and also on political, economic and informational areas.

The ideal response to the risks generated by cryptocurrencies for national security would be a coordinated international effort to regulate their use and prevent hostile parties of using them in ways that would affect the national security. In reality, such an effort is hindered by lack of awareness, the complexity of the issues, the novelty of the cryptocurrency concept and many other factors. At national level, significant efforts should be made to regulate the sector, starting with developing and enforcing legislation regarding the nature, use, and taxation of cryptocurrencies. The already existing Anti Money Laundering / Know Your Customer legislation should be extended to cover the functioning of cryptocurrencies exchanges, digital wallets and of the companies accepting cryptocurrencies as a mean of payment. The structures in the National Defence, Public Order and National Security System should also adapt their regulations, activities, and personnel training to counter the new ways

[29] Zheping Huang, *China, home to the world's biggest cryptocurrency mining farms, now wants to ban them completely*, 2019, https://www.scmp.com/tech/policy/article/3005334/china-home-worlds-biggest-cryptocurrency-mining-farms-now-wants-ban, accessed on 02 August 2020.
[30] URL: http://www.ndrc.gov.cn/yjzx/yjzx_add_fgs.jsp?SiteId=318, accessed on 02 August 2020.

in which cryptocurrencies could be used by criminal or terrorist organizations, but also by hostile state actors.

The cryptocurrency sector is extremely dynamic, as a result authorities have to adopt a flexible approach to respond coherently to the challenges that arise, but there are numerous challenges in this respect, deriving from bureaucratic inertia and the complexity of the domain, which requires the collaboration between different state structures.

BIBLIOGRAPHY:

1. BAYDAKOVA, Anna, *Millions in Crypto Is Crossing the Russia-China Border Daily, Tether Is King*, 2019, https://www.coindesk.com/tether-usdt-russia-china-importers, accessed on July 04, 2020.
2. BOAZ, David, 2019, *The fundamentals of the theory of liberty*, Libertarianism.org, https://www.libertarianism.org/essays/what-is-libertarianism
3. COLUMBIA, David, *The Politics of Bitcoin: Software as Right-Wing Extremism. of Bitcoin: Software as Right-Wing Extremism*, Quinn DuPont, 2017.
4. CUEN, Leigh, *Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report*, 2019, https://www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report
5. HARMAN, Danna, *U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*, Haaretz, 2015, http://www.haaretz.com/middle-east-news/.premium-1.639542
6. HUANG, Zheping, *China, home to the world's biggest cryptocurrency mining farms, now wants to ban them completely*, 2019, https://www.scmp.com/tech/policy/article/3005334/china-home-worlds-biggest-cryptocurrency-mining-farms-now-wants-ban
7. MUELLER, Robert, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Washington, D.C. March 2019, https://www.justice.gov/storage/report.pdf
8. MUNRO, Andrew, *Privacy cryptocurrency among "greatest national security threats" Secret Service says*, https://www.finder.com.au/privacy-cryptocurrency-among-greatest-national-security-threats-secret-service-says
9. NADEAU, Michael, *What is cryptojacking? How to prevent, detect, and recover from it*, 2020, https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
10. NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf
11. SCHUEFFEL, Patrick, *The Concise Fintech Compendium*, pg.9, Fribourg: School of Management, 2017, Fribourg, Switzerland, http://schueffel.biz/wp-content/uploads/2017/09/Schueffel-2017-The-Concise-FINTECH-COMPENDIUM.pdf
12. TAYLOR, Adam, *The Islamic State (or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin*, The Washington Post, 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamicstate-or-someone-pretending-to-be-it-is-trying-to-raisefunds-using-bitcoin/?utm_term=.17ae7b7b7 221
13. YUNIAR, Resty Woro, *Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says*, The Wall Street Journal, 2017, http://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198

CYBER ACTIVITIES IN THE GREY ZONE: AN OVERVIEW OF THE RUSSIAN AND CHINESE APPROACHES

Guillem COLOM-PIELLA, Ph.D.
Professor of Political Science, Pablo Olavide University, Seville, Spain.
E-mail: gcolpie@upo.es

Abstract*: Concepts such as "hybrid threat" or "grey zone" are used to define the wide range of "political warfare" actions that countries such as Russia, China, Iran or North Korea employ for projecting their influence, plausibly denying their responsibility and hampering any response by not crossing the threshold of an armed conflict. Those characteristics allow many actors to project their power asymmetrically by hindering the attribution of their actions, preventing the allocation of legal responsibilities, making retaliation more difficult and compromising the credibility of deterrence. Although many of these actions are carried out in the physical world, the virtual domain seems the natural realm for these activities. This is due to the ambiguity, anonymity, asymmetry, economy and ubiquity of cyberspace. This contribution focuses on the "grey zone" activities in the cyber and information domains conducted by two relevant powers – China and Russia – and discuss the problems and prospects related to those.*

Keywords: *hybrid threat; grey zone; cyber warfare; information warfare; China; Russia.*

Introduction[1]

Despite their theoretical, historical and practical limitations[2], the concepts *hybrid threat* or *grey zone* have become popular in the Western military jargon. They are used for describing the activities of countries such as Russia, China, Iran or North Korea, among others, to project their influence, plausibly denying their responsibility and hindering the opponent's response while avoiding crossing the threshold of armed conflict.[3]

The *grey zone*, broadly defined as the space that separates peace from war is, by nature, ambiguous. This ambiguity is what allows revisionist powers such as the above described to project their power beyond their borders knowing that, if their activities can be

[1] *This contribution is part of the research project Ciberataques y gobernanza global (DER2017-85612-R) (Ministerio de Economía, industria y competitividad) (2018-21).*

[2] For an overview of those limitations, see: Donald Stroker & Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War – Two Failures of American Strategic Thinking", *Naval War College Review*, 2020, 73-1, pp. 1-37; or Antulio Echevarria, *Operating in the Gray Zone: an Alternative Paradigm for U.S. Military Strategy*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2016.

[3] There are plenty of potential or ongoing *grey zones* – ranging from white-grey to black grey – mainly in the Russian or Chinese spheres of influence. In this sense, one interesting aspect that has been traditionally neglected is the relationship between the development of a *grey zone* and the consolidation of the so-called *Anti-Access/Area-Denial* (A2/AD) that could change the strategic calculus of the different parties and, thus, erode the military and escalation dominance. The following work provides some insights that could not only be applied in the Chinese scenario, but also be theoretically developed in the future (Michael Johnsson; Robert Dalsjö (eds.), *Beyond Bursting Bubbles – Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction*, FOI, Stockholm, 2020).

plausibly denied and they do not affect the vital interests of the victim, they may hardly have a clear and effective response.[4]

Isolated, these actions that may include support for political opposition, economic coercion, influence activities, cyberattacks, aggressive intelligence, coercive deterrence or *fait accompli* policies will hardly constitute a *casus belli* because they will always be placed below the threshold of an armed conflict.[5] However, its added long-term effect by using "salami tactics"[6] – combining actions that provide small gains – could alter the existing correlation of forces.[7] Related to those issues, another important characteristic of a *grey zone* is the fact that erodes traditional deterrence since the low profile activities performed, their plausible deniability and the interests at stake cannot justify an escalation … at least to some extent. In fact, the elimination of general Qasem Soleimani with no escalatory effects (at least until now)[8] seem to demonstrate that an actor cannot only restore deterrence by climbing a step in the escalation ladder, but also restore the strategic initiative and make a *grey zone* disappear, at least temporarily.[9]

Consequently, this grey area separating peace from war is the natural ground for the traditional political warfare activities. Those use all the State's power instruments short of war to weaken, influence and demoralize politically, militarily, economically or socially the adversary[10]. These multidimensional strategies are, precisely, what are currently known as *hybrid threats*.[11] Therefore, a *grey zone* situation is a conflicting peace contrary to the *bona fide* principles that are supposed to define international relations, to the point of being a

[4] Take, for example, the institutional and political paralysis after the Estonia cyberattacks of 2007 or the lukewarm response taken by the United States against the Russian Federation's interference in the 2016 presidential elections. In the latter case, it was based on the expulsion of Russian diplomats; an act of retaliation with a marked political character but without any significant effects for the Kremlin.

[5] However, a *grey zone* could precede a situation of war, since it could be used for establishing the preconditions for launching a military operation. In this sense, one of the main issues when thinking in *grey zones* is how to discover that one actor is entering in such a situation.

[6] Robert Haddick, "Salami Slicing in the South China Sea: China's slow, patient approach to dominating Asia". *Foreign Policy*, 3 August 2012, URL: https://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/, accessed on 25 August 2020.

[7] For a general overview of the concept see: Javier Jordán, "El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo", *Revista Española de Ciencia Política*, 48/2018, pp. 129-151; Hal Brands, *Paradoxes of the Gray Zone*, Foreign Policy Research Institute, Philadelphia, 2016; Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2015; Lyle Orris et al., *Gaining Competitive Advantage in the Gray Zone. Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica, RAND Corporation, 2019 or Michael Green, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Center for Strategic and International Studies, Washington DC, 2017.

[8] Ethan Bueno, "The U.S. Can Deter Iran but Not Its Proxies, *Foreign Policy*, 23 January 2020, URL: https://foreignpolicy.com/2020/01/23/united-states-iran-proxies-deterrence-suleimani/, accessed on 28 August 2020; Daniel Byman, "Is deterrence restored with Iran?", *The Brookings Institution*, 16 January 2020, URL: https://www.brookings.edu/blog/order-from-chaos/2020/01/16/is-deterrence-restored-with-iran/, accessed on 28 August 2020.

[9] In this sense, maybe the conventional military balance between the parties is an important aspect for assessing the success of a *grey zone*. If the actor developing a *grey zone* also maintains military superiority, it will likely maintain the scalation dominance in any scenario. This issue – and its effects in the information environment – should be studied with more detail.

[10] Linda Robinson et al. *Modern Political Warfare. Current Practices and Possible Responses*, RAND Corporation, Santa Monica, 2018.

[11] Remember that, originally, the concept of *hybrid war* or *hybrid warfare* was used to define *"…a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."* (Frank Hoffman, *Conflict in the 21st Century: the rise of hybrid wars*, Potomac Institute for Policy Studies, Arlington, 2007, p. 14).

complete new category between situations of "authentic" peace and war.[12] Consequently, the *grey zone* concept allows us to improve the analysis of the great power competition in the context of the so-called "fog of peace" because its ambiguity.[13]

Although many of these activities are carried out in the physical world (from the traditional incursions of Chinese fishermen into the disputed islands with Japan to the attacks on Saudi tankers in the Persian Gulf), a growing number of activities are performed in the virtual domain. This is due to the ambiguity, anonymity, asymmetry, economy and ubiquity that characterize cyberspace. These features allow many actors to project their power asymmetrically by hindering the attribution of their actions, preventing the allocation of legal responsibilities, hampering any retaliation and compromising credibility of the deterrent tools of the victim.

Initially, the cyberattacks coming from Russian territory against Estonia (2007) and Georgia (2008) or the Chinese cyberespionage (which led to the famous attribution of the *Advanced Persistent Threat 1* (APT-1) in 2013),[14] led the Western powers to focus on the exploitation activities and the potential disruptive effects that a cyberattack could have against their services, systems and networks. Hence the interest of the international community in determining what kind of cyberattack might constitute a *casus belli* and in developing a "classical" approach to deterrence by denial and punishment. However, the expansion of Daesh in Iraq, Iran or Yemen, the occupation of Crimea, the war in eastern Ukraine or the information operations in the 2016 U.S. presidential elections demonstrated that the online environment also allowed the conduct of lower profile activities equally capable to affect national security while violating the established legal principle of non-intervention in domestic affairs. Also, the disinformation and misinformation activities – conducted in parallel with the propaganda campaigns for supporting the Russian and Chinese humanitarian aid – carried out by Moscow, Beijing and Teheran during the COVID-19 pandemics may have a much lower profile and do not directly harm national security, but they can also be regarded as the new normal in the *grey zone*.[15]

Multi-channel propaganda, user profiling to reinforce the filter-bubble, dissemination of fake news or leaking compromised personal information could also be used to exploit existing divisions in societies and influence their public opinions. In addition, the Russian campaigns in Crimea, Ukraine or Syria not only highlighted the relevance of electronic warfare in modern conflicts, but also demonstrated the potential use of the radio space for interfering communications, degrading air defence systems, spoofing GPS signals or obstructing intelligence activities.[16]

What do computer network exploitation, defence or attack operations, cyberspace-influence operations, electronic warfare activities have in common? All of them are waged in the information space, which encompasses cyberspace, and whose effects can be observed in the logical, physical and cognitive spheres. The information space as a new domain of war

[12] Nadia Schadlow, "Peace and War: the Space between", *War in the Rocks*, 18 August 2014, URL: https://warontherocks.com/2014/08/peace-and-war-the-space-between/, accessed on 28 August 2020.
[13] Emily Goldman, *Power in Uncertain Times. Strategy in the Fog of Peace*, Stanford University Press, Stanford, 2006.
[14] Mandiant, *APT-1. Exposing one of China's Cyber Espionage Units*, Mandiant, Alexandria, 2013, URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, accessed on 29 August 2020.
[15] Betsy Woordruff, "State report: Russian, Chinese and Iranian disinformation narratives echo one another", *Politico*, 21 April 2020, URL: https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107, accessed on 30 August 2020.
[16] Neglected since the end of the Cold War, electronic warfare has experienced a revival not only after the Russian activities in Crimea, Ukraine or Syria, but also because of the growing convergence between cyber and radio space. This has led to the development of the concept of *Cyberspace Electro-Magnetic Activities* (CEMA).

became popular with the rise of the Revolution in Military Affairs (RMA)[17] in the early 1990s. However, at the end of the decade it was replaced – perhaps by the global penetration of the internet, its impact on the world economy or the growing reliance on the services and infrastructures that enabled it – by cyberspace as an eminently technical domain and as a fifth domain of war ... at least for the West.

Due mainly to their historical and political heritage, both Russia and China understand that information is a relevant tool for projecting their national power and one of the pillars of national sovereignty, but also one of the main assets to maintain their political, social or moral stability against harmful external influences. These conceptions that focus on the protection of the national information space and the projection of influence abroad – something that was traditionally done via political propaganda – precede the Internet. However, in the 1990s both countries warned that new technologies and the chances of the population gaining different sources of information were not only a security threat because of their destabilizing potential, but also because of their technological dependence to the United States.

As a result, they not only considered it necessary to restrict access to the internet and to try to get the international community to support its control and regulation to protect national security, but also to create its own and potentially cyber/information ecosystem isolated from the rest of the world[18]. At the same time, their military strategists understood that information – and not the smart weapons initially assumed by the West in the midst of this revolutionary euphoria – could be the mainstay of this RMA that promised to transform war.[19] Consequently, they assumed that the information warfare would be one of the pillars of their military transformations, the foundation of future conflicts and the general framework where not only cyberspace is located, but the environment where any activity is carried out physics, logic and cognitive linked to the use of information as a vector, target or medium.

In addition, both countries – whose conceptions of information warfare have important similarities but also significant differences[20] – have successfully integrated information activities into multidimensional strategies to project their power and national interests in the *grey zone*. Having these elements in mind, this contribution to the conference will briefly explain how Russia and China conceive information warfare and how they use it in the *grey zone* of the conflict.

1. Russian information warfare

Russia conceives information warfare (*informatsionnaya voyna*) as one of the pillars of the "new generation wars" and the foundation of future conflicts.[21] Based on various

[17] The RMA popularized the concept of information warfare, capable of damaging, degrading or destroying the adversary's information systems to paralyze or confuse their decision-making cycle or paralyze their ability to fight. This idea culminated in the Command and Control Warfare (C2W) concept, which would use electronic warfare, psychological operations, operational security and deception to degrade the adversary's decision-making processes (Guillem Colom-Piella, *Entre Ares y Atenea, el debate sobre la Revolución en los Asuntos Militares*, Instituto Universitario General Gutiérrez Mellado, Madrid, 2008).

[18] Samuel Bendett, Elsa Kania, *A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry*, Australian Strategic Policy Institute, Canberra, 2019.

[19] For the Russian case, Makmut Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Frank Cass, London, 1998; and for the Chinse one: Qiao Liang; Wang Xiangsui, *Unrestricted warfare: China's master plan to destroy America*, Filament Books, New York, 2004.

[20] Jake Wallis, "China and Russia aren't the same when it comes to information warfare", *The Strategist*, 25 September 2019, URL: https://www.aspistrategist.org.au/china-and-russia-arent-the-same-when-it-comes-to-information-warfare/, accessed on 30 September 2020.

[21] Sergei Chekinov; Sergei Bogdanov, "The Nature and Content of a New-Generation War", *Military Thought* (English edition), 4/2013, pp. 12-22.

traditions – from the military *maskirovka*, the Soviet active measures, the communist subversion or the reflexive control theories – and developed within the framework of the RMA, the Russian information warfare is widely debated both inside and outside the country. Although several official sources refer to the concept and the basic doctrine of the armed forces highlights its importance, the specific doctrine remains classified and its information warfare remains surrounded by a halo of mystery.

Although there are a number of official definitions, the most popular considers it to be *"…the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force"*.[22] Considered by many strategists as a component of a global information confrontation in which the West wants to impose its will without resorting to direct military confrontation, information warfare serves is a "hybrid" tool that goes much further than disinformation, fake news or cyberattacks.[23]

Western chronicles underline its use as an asymmetric weapon in the *grey zone* while highlighting techniques such as reflexive control (or the manipulation of the decision-making processes), manipulation of the public opinion to accept the Russian actions, or the traditional subversion or destabilization activities. However, Moscow understands that information warfare can serve both to achieve strategic-political objectives without the need to use military force and contribute to the conduct of military operations.[24] Used in peacetime, escalation and open conflict at the strategic, operational and tactical levels, information warfare has an offensive side, focused on achieving informational superiority over the adversary, and defensively, for ensure the country's information security and thus contribute to strategic stability.[25]

In addition, assuming that the information environment comprises everything related to information and that any channel, medium or physical, digital or cognitive vector can be destroyed, degraded, altered or corrupted, any technology, means or activity that has an informational dimension can become an information weapon. Consequently, the shutdown of an air defence system, the destruction of a communications station, the spoofing of a GPS signal, the denial of a website, the exfiltration of personal information, the assassination of a journalist, an official statement, a hoax on *Whatsapp*, a digitally altered image on *Instagram* or a meme on *Twitter* are some of the weapons that can be used to fight on the information spectrum. Combined, these will be geared towards the achievement of *information-technical* effects on the enemy infrastructures and systems and *information-psychological* on their perceptions. To this end, it is assumed that Russia can use a wide variety of tools, some of which are similar to those used in Western doctrine (electronic warfare, psychological operations, intelligence, deception or cyberoperations) and others linked to the traditional soviet-style *active measures* (social control, misinformation, information manipulation,

[22] Russian Ministry of Defence, *Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space*, Russian Ministry of Defence, 2011, art. 1.

[23] Also, when thinking in information confrontations, one could also stress all the narratives related to the origins, development, management and vaccines of the COVID-19 (Sergey Sukhankin, "COVID-19 As a Tool of Information Confrontation: Russia's Approach", *The School of Public Policy Publications*, No. 3/2020, p. 13, URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3566689_code1646523.pdf?abstractid=3566689&mirid=1, accessed on 29 August 2020).

[24] Jonas Kjellèn, Jonas, *Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces*, FOI, Stockholm, 2019.

[25] Charis Saifetdinov, "Informatsionnoe protivoborstvo v voennoi sfere", *Voennaia mysl*, 7/2014, pp. 38-41.

blackmail, extortion or pressure in the media and on social media).[26] Depending on whether Russia is in peace, *grey zone* or war, the Kremlin will use different vectors more or less openly to ensure its information security, to maintain the strategic balance, to shape public opinion, to weaken the will of the opponent or to achieve informative superiority with all means.

In conclusion, Moscow understands that information warfare is a major factor in the global geopolitical confrontation and a comprehensive activity that requires the participation of a wide range of actors. Although it can be used across the conflict spectrum, perhaps it is in the *grey zone* where it can achieve its full potential, masking its origins and hindering its attribution while supporting the achievement of its foreign policy objectives without resulting in military escalations with unpredictable consequences.

2. Chinese information warfare

Like Russia, China also perceives information warfare (*xinxi zhan*) as one of the pillars of modern conflicts, a crucial component of the "three" future wars (non-contact, non-linear and asymmetric) and one of the core competencies the People's Liberation Army (PLA). Initially based on the emulation of American concepts[27], the Chinese information warfare has been developing since the 1990s.

Assuming that, in the Information Age, national power is measured in informational terms, Chinese leaders concluded a quarter of a century ago that the rise and fall of powers would be determined by the ability to generate, obtain, transmit, analyse and exploit information. As a result, China had to adapt to the Information Age by supporting its national development (thus legitimizing the Chinese Communist Party), creating its own ecosystem of technological innovation, and preparing the PLA for informatized war (*xinxihua zhanzheng*). This transformation, whose pillars were laid by Premier Yang Zemin following the victory of the U.S.-led coalition in the Operation Desert Storm, would be achieved by reducing its forces, mechanizing its units and computerizing their processes. This would allow the country to effectively combat in "local wars under high-tech environments" and, after, in "local wars under informatized environments"[28].

Based on a number of traditions – information warfare, political warfare, revolutionary war or the teachings of Sun Tzu and Mao Tse-Tung[29] – and developed in line with the so-called RMA with Chinese characteristics[30], Chinese information warfare is subject of important debates outside the country. Although there is abundant foreign literature and various official and informal sources of the country have been referring to the concept since the 1990s, military doctrine remains classified and its information war remains an unknown for the Western strategists. Many focus their interest on cyberoperations – defined by China

[26] Ulrike Franke, *War by non-military means. Understanding Russian Information Warfare*, FOI, Stockholm, 2015.
[27] However, it is possible to find a Chinese book from 1985 that related the information revolution with the development of information warfare (James Mulvenon; Richard Yang (eds.), *The People's Liberation Army in the Information Age*, RAND Corporation, Washington DC, 1999, p. 177).
[28] To understand these changes, it is advisable to read the following book: Joe McReinolds (ed.), *China's Evolving Military Strategy*, The Jamestown Foundation, Washington DC, 2017.
[29] Robyn Ferguson, *Information Warfare with Chinese Characteristics: China's Future of Information Warfare and Strategic Culture*, U.S. Army Command and General Staff College, Fort Leavenworth: 2011.
[30] Jacqueline Newmeyer, "The Revolution in Military Affairs with Chinese Characteristics", *Journal of Strategic Studies*, 4/2010, 33, pp. 483-504. In fact, General Wang Pufeng – considered as the father of the Chinese information warfare – linked those ideas in 1995 (Wang Pufeng, *Xinxi zhanzheng yu junshi geming*, Junshi Kexueyuan, Beijing, 1995).

as network warfare (*wangluo zhan*) – psychological operations or denial and deception activities, underlining its asymmetrical nature and discussing whether it would allow it to succeed in conflicts without the need to fight hand-to-hand[31]. However, China's information warfare seems more complex and comprehensive.

The military terminological dictionary of the PLA defines information warfare as *"*[those] *activities carried out by the contenders in the information domain. It includes the protection of information resources, the achievement of the initiative in the production, transmission and management of information or the disruption of the adversary's ability to transmit information in order to establish the necessary conditions to deter, combat and win conflicts."*[32]. The attainment of these objectives require the conduction of a wide range of physical, logical and cognitive activities at the political (fighting the so-called three wars: psychological, legal (*lawfare*) and public opinion warfare)[33] and military (through electronic warfare, network warfare, psychological warfare, command and control warfare and intelligence warfare) levels to achieve the information supremacy. While the planning of the former falls to the Central Military Commission of the Chinese Communist Party, the Strategic Support Force of the PLA executes the latter. However, the same nature, ubiquity, interconnection and variety of actors interacting in the information environment requires that these actions must be carried out both in peacetime and in a period of war, and both against military and civilian objectives[34]. As a result, Chinese strategists understand that those activities – from psychological operations, political propaganda and *lawfare* to penetrating foreign networks for detecting vulnerabilities – must be carried out against the whole society both in peacetime and before the start of hostilities.

In other words, by blurring the border between peace and war by establishing – at least for our conception – a wide *grey zone* overlapping peaceful competition, China considers it legitimate to employ multiple psychological, propaganda, electronic or cyber activities for supporting the achievement of information advantage in crisis and war, but also supporting national development in all of its dimensions[35].

To carry out these tasks, the Chinese information warfare approach combines defence, exploitation and offensive activities, the protection of its own informational resources[36] and information deterrence. Combining deterrence, persuasion and coercion, the Chinese approach to deterrence (*weishe*) uses the global dependence on the internet to demonstrate its informative advantage and the potential effects of any escalation. Moreover, while its information activities on social media are generally less active, sophisticated and

[31] Toshy Yoshinara, *Chinese Information Warfare. A phantom menace of emerging threat?*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks: 2001.

[32] Academy of Military Science of the Chinese People's Liberation Army, *Chinese People's Liberation Army Military Terminology*, AMS Publishing House, Beijing, 1997, pp. 764-766.

[33] Those political warfare activities *"…strive to shake the enemy's will, question their motives, induce divides and splits within the enemy's ranks, and constrain their activities […] erode an adversary's will and thus reduce the ability to sustain any resistance to more kinetic operations."* (Dean Cheng, *Cyber dragon: Inside China's information warfare and cyber operations*, Praeger, Santa Barbara, 2017, p. 42).

[34] Larry Wortzel, *The Chinese People's Liberation Army and Information Warfare*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2014.

[35] As a consequence, the Chinese industrial cyberespionage – carried out by PLA units – not only needs to be understood as a means for obtaining relevant information for the national development, but also as a tool for gaining knowledge of the potential adversary (Derek Johnson, "How China uses cyber theft and information warfare", *Federal Computer Week*, 6 May 2019, URL: https://fcw.com/articles/2019/05/06/china-information-warfare-dod-report.aspx, accessed on 30 August 2020).

[36] It also means protecting its population from any external interference that may damage the legitimacy of the Chinese Communist Party (Cheng, *op. cit*., pp. 53-78 or Michael Mazarr et al., *Hostile Social Manipulation. Present Realities and Emerging Trends*, RAND Corporation, Santa Barbara, 2019, pp. 105-166).

strategically-oriented than the Russian ones, it should not be forgotten that they are especially active both domestically and in its area of direct influence[37]. However, there is the possibility that the lessons identified by Moscow in Crimea, Ukraine or Syria campaigns might be used by Beijing to expand its capabilities in this domain, as the information-related activities during the outbreak of the COVID-19 may suggest[38].

Conclusions

The *grey zone* is ambiguous because of lack of a legal regulation and the difficulty to adapt the existing norms to this "new" reality. This ambiguity is what allows any power not satisfied with the current *status quo* to employ multidimensional strategies – now popularized as *hybrid threats* – to project their power by plausibly denying their authorship, degrading deterrence and strengthening their relative position in the global sphere.

Although many of these activities are carried out in the physical world, many are performed in the virtual domain aiming at effecting the physical, logical or cognitive dimensions. Although the Chinese and Russian approaches have important similarities (from their traditions linked to controlling information, their interpretation of the RMA, a lesser technocentric approach to the information domain than the West), they also show significant differences motivated by their strategic culture, political tradition or technical capacity. In this sense, the Russian information warfare in the lower part of the *grey zone* seems to adapt the Soviet active measures to the online environment; in the upper part, it is more militarized. On the other hand, China's information warfare in the *grey zone* seems to be more focused on propaganda and *lawfare*, computer network exploitation activities through APTs against foreign countries to support national development and information deterrence activities – perhaps including GPS spoofing[39] – to demonstrate the Chinese capabilities in this domain. In any case, both countries understand that information warfare is more than cyberwarfare, that it can be used across the conflict spectrum, that it can be integrated into multidimensional strategies, that it can be integrated into hybrid tactics and that it is much more than propaganda, disinformation, cyberattacks or the use of *trolls* and *bots* on social media.

BIBLIOGRAPHY:

1. ACADEMY OF MILITARY SCIENCE OF THE CHINESE PEOPLE'S LIBERATION ARMY, *Chinese People's Liberation Army Military Terminology*, AMS Publishing House, Beijing, 1997.
2. BENDETT, Samuel; KANIA, Elsa, *A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry*, Australian Strategic Policy Institute, Canberra, 2019.
3. BRANDS, Hal, *Paradoxes of the Gray Zone*, Foreign Policy Research Institute, Philadelphia, 2016.

[37] Mazarr, *op. cit*., pp. 113-126. For the aspects related to the Hong Kong protests, see: Tom Uren; Elise Thomas; Jacob Wallis, *Tweeting through the Great Firewall*, International Cyber Policy Centre – Australian Strategic Policy Institute, Canberra, 2019.

[38] Jessica Brandy; Torrey Taussig, "The Kremlin's disinformation playbook goes to Beijing", *The Brookings Institution*, 19 May 2020, URL: https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/, accessed on 30 August 2020.

[39] Christopher Woody, "The Navy's 4th accident this year is stirring concerns about hackers targeting US warships", *Business Insider*, 24 August 2017, URL: https://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?IR=T, accessed on 30 august 2020.

4. BRANDT, Jessica; TAUSSIG, Torrey, "The Kremlin's disinformation playbook goes to Beijing", *The Brookings Institution*, 19 May 2020, https://www.brookings.edu/blog/ order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.
5. BUENO, Ethan, "The U.S. Can Deter Iran but Not Its Proxies, *Foreign Policy*, 23 January 2020, https://foreignpolicy.com/2020/01/23/united-states-iran-proxies-deterrence-suleimani/
6. BYMAN, Daniel, "Is deterrence restored with Iran?", *The Brookings Institution*, 16 January 2020, https://www.brookings.edu/blog/order-from-chaos/2020/01/16/is-deterrence-restored-with-iran/.
7. CHAMBERS, John, *Countering Gray-Zone Hybrid Threats*, Modern War Institute, West Point, 2016.
8. CHEKINOV, Sergei; BOGDANOV, Sergei, "The Nature and Content of a New-Generation War", *Military Thought* (English edition), 4/2013.
9. CHENG, Dean, *Cyber dragon: Inside China's information warfare and cyber operations*, Praeger, Santa Barbara, 2017.
10. COLOM-PIELLA, Guillem, *Entre Ares y Atenea, el debate sobre la Revolución en los Asuntos Militares*, Instituto Universitario General Gutiérrez Mellado, Madrid, 2008.
11. ECHEVARRIA, Antulio, *Operating in the Gray Zone: an Alternative Paradigm for U.S. Military Strategy*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2016.
12. FERGUSON, Robyn, *Information Warfare with Chinese Characteristics: China's Future of Information Warfare and Strategic Culture*, U.S. Army Command and General Staff College, Fort Leavenworth, 2011.
13. FRANKE, Ulrike, *War by non-military means. Understanding Russian Information Warfare*, FOI, Stockholm, 2015.
14. GAREEV, Makhmut, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Frank Cass, London, 1998.
15. GOLDMAN, Emily, *Power in Uncertain Times. Strategy in the Fog of Peace*, Stanford University Press, Stanford, 2006.
16. GREEN, Michael, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Center for Strategic and International Studies, Washington DC, 2017.
17. HADDICK, Robert, "Salami Slicing in the South China Sea: China's slow, patient approach to dominating Asia". *Foreign Policy*, 3/2018, https://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/
18. HOFFMAN, Frank, *Conflict in the 21st Century: the rise of hybrid wars*, Potomac Institute for Policy Studies, Arlington, 2007.
19. JOHNSON, Derek, "How China uses cyber theft and information warfare", *Federal Computer Week*, 6 May 2019, https://fcw.com/articles/2019/05/06/china-information-warfare-dod-report.aspx
20. JONSSON, Michael; DALSJÖ, Robert (eds.), *Beyond Bursting Bubbles – Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction*, FOI, Stockholm, 2020.
21. JORDÁN, Javier, "El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo", *Revista Española de Ciencia Política*, 48/2018, pp. 129-151.
22. KJELLÈN, Jonas, *Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces*, FOI, Stockholm, 2019.
23. LIANG, Qiao; XIANGSUI, Wang, *Unrestricted warfare: China's master plan to destroy America*, Filament Books, New York, 2004.
24. MANDIANT, *APT-1. Exposing one of China's Cyber Espionage Units*, Mandiant, Alexandria, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
25. MAZARR, Michael et al., *Hostile Social Manipulation. Present Realities and Emerging Trends*, RAND Corporation, Santa Barbara, 2019.
26. MAZARR, Michael, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2015.
27. MCREINOLDS, Joe (ed.), *China's Evolving Military Strategy*, The Jamestown Foundation, Washington DC, 2017.

28. MORRIS, Lyle et al., *Gaining Competitive Advantage in the Gray Zone. Response Options for Coercive Aggression below the Threshold of Major War*, Santa Monica, RAND Corporation, 2019.
29. MULVENON, James; YANG, Richard (eds.), *The People's Liberation Army in the Information Age*, RAND Corporation, Washington DC, 1999.
30. NEWMEYER, Jacqueline, "The Revolution in Military Affairs with Chinese Characteristics", *Journal of Strategic Studies*, 4/2010, 33.
31. PUFENG, Wang, *Xinxi zhanzheng yu junshi geming*, Junshi Kexueyuan, Beijing, 1995.
32. ROBINSON, Linda et al. *Modern Political Warfare. Current Practices and Possible Responses*, RAND Corporation, Santa Monica, 2018.
33. RUSSIAN MINISTRY OF DEFENCE, *Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space*, Russian Ministry of Defence, 2011.
34. SAIFETDINOV, Charis, "Informatsionnoe protivoborstvo v voennoi sfere", *Voennaia mysl*, 7/2014.
35. SCHADLOW, Nadia, "Peace and War: the Space between", *War in the Rocks*, 18 August 2014, https://warontherocks.com/2014/08/peace-and-war-the-space-between/
36. STROKER, Donald; WHITESIDE, Craig, "Blurred Lines: Gray-Zone Conflict and Hybrid War – Two Failures of American Strategic Thinking", *Naval War College Review*, 1/2020, 73.
37. SUKHANKIN, Sergey, "COVID-19 As a Tool of Information Confrontation: Russia's Approach", *The School of Public Policy Publications*, 3/2020, p. 13, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3566689_code1646523.pdf?abstractid=3566689&mirid=1
38. UREN, Tom; THOMAS, Elise; WALLIS, Jacob, *Tweeting through the Great Firewall*, International Cyber Policy Centre – Australian Strategic Policy Institute, Canberra, 2019.
39. WALLIS, Jake, "China and Russia aren't the same when it comes to information warfare", *The Strategist*, 25 September 2019, https://www.aspistrategist.org.au/china-and-russia-arent-the-same-when-it-comes-to-information-warfare/
40. WOODY, Christopher, "The Navy's 4th accident this year is stirring concerns about hackers targeting US warships", *Business Insider*, 24 August 2017, https://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?IR=T
41. WORTZEL, Larry, *The Chinese People's Liberation Army and Information Warfare*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2014.
42. YOSHINARA, Toshi, *Chinese Information Warfare. A phantom menace of emerging threat?*, Strategic Studies Institute – U.S. Army War College, Carlisle Barracks, 2001.

REORGANIZING THE ECONOMIC ENVIRONMENT THROUGH ANTIFRAGILITY AND COMPETITIVE INTELLIGENCE

Adina MIHĂESCU
PhD Student, Doctoral School of International Relations and Security Studies, Babes Bolyai University, Cluj Napoca, Romania. E-mail: adinamihaescu12@gmail.com

Elena-Iuliana BULGARIU
PhD Student, Doctoral School of International Relations and Security Studies, Babes Bolyai University, Cluj Napoca, Romania. E-mail: ebulgariu@gmail.com

Abstract*: Throughout time, the political, cultural, economic revolutions, the innovations - the evolution in general - are based on the capacity shown by the societies, and by the system in their ensemble, to absorb the shocks and, even more than that, to evolve and to improve themselves as a result. If the resilience is referred to the ability to face and to resist the unfavorable situations that have risen, the antifragility requires, also, a fast accommodation which, inevitably, brings progress together with it. Anticipating the evolutions and the fast transformations which appeared within the markets, or the various industries, represents challenges that the companies' managers find harder and harder to manage. Starting from certain given situations, formulating the (short, middle and long-term) strategies represents a major step on which the survival of the company itself depends. More than ever, the economic environment, which is continuously changing and globalizing, needs precise and updated information, their analysis and pertinent predictions, and this, mainly, the task carried out by the Competitive Intelligence field. This article aims at transposing the concept of antifragility within the economic environment, directly connected with the field of business information and to relate these systemic concepts, highlighting how they can bring additional value and help decreasing the risks and bringing to a sustainable economic progress.*

Keywords*: antifragility; resilience; competitive intelligence; economic intelligence; economic security.*

Introduction

The term of *economic intelligence* was first used in large corporations in the United States, which created, influenced by the model of military intelligence during World War II, intelligence departments specializing in sales (1960s), and, since the 1970s, the first structures that dealt with what is today known as *competitive intelligence* (CI). The introduction of economic intelligence systems was perceived as a measure of vital importance for developing countries, but the studies of experts at that time did not generate a dynamic in the sense of its adoption, due to disparities between states, different stages of development and implementation of national development projects and local information cultures. To these factors were added technological and information inequalities, the growing dependence on knowledge and the tendency to exclude poor states, in which information collection and processing systems were characterized by unreliability, especially in relation to local environments, such as the lack of quality information, adapted to the economic and technological realities, respectively to the real needs at national level.

Therefore, economic intelligence has been considered an effective model for accelerating the development of poor states and balancing their power to negotiate, to relate, in the context of global power balance.

1. Economic intelligence from the point of view of state actors

The United States is the space in which *economic intelligenc*e developed on a wide scale, as a true doctrinal culture. The two factors causing this trajectory are:

- The American power's main role in developing market economy;
- The systemic way in which the knowledge circumscribed to economic intelligence has been integrated with management elements and was spread within the administrative segment[1].

In this way, the economic intelligence has, also, become a research subject within the management training programs, especially as a result of Michael Porter's contribution at the beginning of the 1980's.[2]

In spite of all these, the American Professor R. E. Freeman has offered in 1984 (*Strategic Management. A stakeholder approach*), a more extended definition and approach to economic intelligence, by assimilating the concept of *shareholders*, with highlight on these entities' influence over the market-delimited environment – government, territorial collectivities, activist' groups, mass media, labor unions, etc.).[3] The stakeholders are, as such, much more dangerous when directly connected with researching strategies in the United States, the notions related to economic intelligence and influence being presented in official Business Management Master within some of the most prestigious American Universities.[4]

The need for such a knowledge management is supported by the continuously changing competitive environment. The issues related to controlling the economic, technological, political, and social information (influences and behaviors) have radicalized themselves once with the restriction on the markets (caused by the economic crises), the political instability (the fall of the Berlin Wall, the Gulf War) and the passage from the Defense's traditional sectors in *dual* formats, in which the military component is evaluated and sized according to the civilian component (the defense's budget have been modified, other resources have been redirected).[5] This radicalization has brought to the appearance of a new knowledge, especially from the point of view of the method, the *Info War*, which appoints protecting its own economy by a country by mobilizing the informational structures (IT infrastructures, capacity to collect, store, process, and spread economic and political information) and developing influence policies connected to the informational war, respectively through spreading information with destabilizing role by key-actors (who concentrate the informative power in their hands).

The new forms of competition bring out the issue of the systemic integration of these new dimension in the analysis of the competitive environments, both in terms of research as well as of forming the future managers.

The Anglo-Saxon concept of economic intelligence was developed in the United States, at the end of the 1960s, especially by Harold Wilensky, who in his reference-book,

[1] Oubrich, Mourad, "L'intelligence économique. Un outil de management stratégique orienté vers le développement de nouvelles connaissances", *La Revue des Sciences de Gestion*, vol. 226-227, no. 4, 2007, pp. 77-88.
[2] Michael, Porter, *Competition in the open economy*, Harvard University Press, 1980.
[3] *Idem* 1.
[4] *Idem* 1.
[5] *Idem* 1.

Organizational Intelligence: Knowledge and Policy in Government and Industry, discuss two major issues:

a. The collective strategies and the cooperation between the government and the companies on generating a common knowledge in order to assure the competitive advantage;

b. The importance of knowledge in economy and industry as a strategic engine for development and change.[6]

In order to insert the concept of economic intelligence, Wilensky identifies four determinants in allotting power, money and time for intelligence (defined as being the systemic collection, interpretation and use of the information in order to reach more strategic purposes) in an organization:

(1) *The level/degree of conflict or competition within an environment related to the degree of involvement or dependence on a government;*

(2) *The internal support and unity organization's degree of dependence;*

(3) *The degree in which the internal operations and the external environment are the object of a trend in management through the possibility of being approached rationally, meaning through foreseeable elements that might be targets of the influence;*

(4) *The organization' size and structure, the heterogeneousness of its members, the diversity of its objectives as well as its centralized authority system*.[7]

Wilensky, especially through his book's title, highlights the fact that the economic intelligence is not a process aimed at accumulating information, but at producing knowledge, by the Government and by the main industrial organizations, including within the collective strategies, if it's the case.

The dependence of each aspect of strategic planning from the economic elements has been, nonetheless, recognized without a doubt. The complex strategic issues associated with testing, deploying, limiting or testing conventional and unconventional forces have implied analyses in which setting the influence exercised by the economic factor (international trade and internal economy) have required a detailed structural modeling and empirical investigations with the purpose of determining certain evolutions. Circumscribed, the importance of the academic environment has, also, been acknowledged, for what is related to the potential for researching, and investigating, certain segments of interest.[8]

While the economy in the defense field implies every form of economic analysis for national security, studying the economic war has been, rather, based on using the economic weapons in the conflicts that took place during the Cold War. These weapons have included sanctions, embargoes, economic attacks aimed at decreasing the enemy' economic potential. The distinction between "defense economics" and "economic warfare" can be relevant in order to determine the economic intelligence as a field of activity and it results from the definitions of the two notions:

- "Defense economics" identifies the application of economic analysis for purposes related to national defense. In the same way in which economy is a science by itself, "defense economics" represents the system-wide study of the options in the case of competitive alternatives, in problems related to expenses, production, effects of the decisions related to macroeconomy, etc., taken in the field of defense industry.

[6] Harold Wilensky, *Organizational Intelligence: Knowledge and Policy in Government and Industry*, Quid Pro Books, 2015.
[7] *Idem*, pp. 88-91.
[8] Shubik, M., Verkerke, J., "Open Questions in Defense Economics and Economic Warfare", *The Journal of Conflict Resolution*, Sage Publications, Inc., Vol. 33, No. 3, 1989, p. 481.

- "Economic warfare" constitutes the use of weapons for strategic purposes, related to oligo-polyism, monopolistic competition, negotiations, and other aspects of competitiveness. In case of economic war, analysts take into account each of the enemy' reactions, and the analysis of self is an ensemble with political, military, and economic considerations not included in the "defense economics" field. [9]

In conclusion, the *economic intelligence* has had, throughout time, two major functions: "weapon" under the shape of "Cold War" which has covered the competition between the two poles – East and West – respectively between the United States and the U.R.S.S.; an essential resource in the competition between the Western states; capitalism, market economy, and everything that has lead us to the actual forms of *business intelligence* and *competitive intelligence.*

2. Economic intelligence from the point of view of non-state actors

Initially used in the military environment, *intelligence* has shown its applicability once with the explosion of information sources and the increase in their accessibility, including in the economic field, as a process with strategic importance destined to generating added value and administrative performance.[10] The improvement brought to accessing the information, eased by the ongoing development of the technologies and of the networks, has started to be considered the key element in the evolution of the economy, particularly for what is related to society in general.

The influence exercised by these factors on the decisional process has reached, as such, the size of a mean that is essential in generating innovative approaches and the responses given by the economic intelligence in relation to the opportunities and the risks set by a world that is changing more and more rapidly. Together with the military intelligence, the economic intelligence has been associated to the purpose of identifying the relevant sources of information, analyzing these information and manipulating them correctly in order to supply the decision-making factors with knowledge.

Based mostly on information available outside of the organization or the state, the application of economic intelligence has started to extend more and more in the sphere of technology, markets and legislation.

The connection and the passing to other domains aimed at studying the means, the techniques, and the methods – like knowledge management and CI – have become evident and, at the same time, complementary, under the conditions set by the development of communications and the expansion of the Internet. The motivation behind this trend was to assure quality information, with strategic value, that can be integrated with data and information used in other domains that are vital for a national economy to function properly. The economic intelligence has become, step by step, the engine of innovation in the process aimed at developing competitiveness.

The fact that the value of the information itself no longer constituted the base for competitive advantage, the context at the beginning of the 1990s imposing to generate and use the information integrated, in order to anticipate the evolutions affecting the social-economic environment, has been accepted on a continuously growing scale.

The *economic intelligence* has consolidated its main status in order to reach a multitude of objectives:

---

[9] *Idem*, pp. 482-483.

[10] Baranga et al., "Trends and Perspectives Regarding the Evolution of the Concept of Economic Intelligence within the Context of the Economic Crisis", *Journal of Knowledge Management*, Economics and Information Technology, Vol. II, Issue 2, 2012, pp. 2-4.

- To describe the competitive environment, to identify the determining factors and elements: the competitors, the products, the request for regulation, the prices, the technologies, etc.;
- The prognosis of the evolution set forth by these factors of competitiveness, including of the technologies with a destructive potential and of the new competitors, etc.;
- The proper monitoring and evaluation of the information technologies;
- Identifying the threats and the weak points, respectively the strong points, and the perspectives for development;
- Establishing a strategy's sustainability and recommending future actions.[11]

Beside collecting data in reference to the competitors, *business competition* has, also, offered a series of operations aimed at protecting and at promoting their own business interests, including security measurements taken against external espionage (counter-espionage in the private sector).

The *business intelligence* has, also, included certain illegal/unethical procedures aimed at affecting a competitor's correct functioning (for example, supplying qualitatively weak products/ materials), but it never extended on the governmental segment, limiting itself to the *business* versus *business* area.[12] The business intelligence, a direct "descendant" of the economic intelligence, is considered to be the most effective method for supplying a full understanding of the economic environment, essential for the decision-makers.

The economic intelligence has started to be practiced in more and more countries and its effectiveness was given by what was thought to be the economic war's main weapon - information and knowledge. The continuously growing volume of data available has created the need for pro-activity in exploiting them, especially in order to respond to the priority transfer from collecting information to how to value them, marking the appearance of what has become the *economy of knowledge*.

The growth of the administrative efficiency in a more and more changing economic environment has become increasingly more important for the development and the consolidation of the national economies, respectively for their safety in relation to threats and crises, whatever their nature. In this way, the aims set forth by the economic intelligence have crystallized in what would have become the base for the future forms of intelligence applied at a national and administrative level – *business intelligence* and *competitive intelligence*:

- Production of useful and relevant information:
- Protecting personal patrimony;
- Influencing the surrounding environment for personal benefit.

The strategic evaluation of the economic environment has become the main axis of the evolution of economic intelligence forms, and information is the raw, useful, and relevant material only under the terms of the correct and safe exploitation. The future has started to be seen in connection with the leaders' capacity to develop aptitudes corresponding to creating and using economic intelligence, to show behaviors adapted to the environment's requirements, competitive aggressiveness and density based on the customer.

The main objective has been the economic intelligence's integrated approach (including from the point of view of the experts from the private and academic environments)

[11] Arenas, E.O., "Strategic intelligence and economic security", in *Strategic Dossier 162 B Economic intelligence in a global world*, Spanish Institute for Strategic Studies, 2014, p. 14.
[12] Johnnson, L., *Secret Agencies. U.S. Intelligence in a hostile world*, Yale University Press 1, 1996 p. 147.

for the purpose of implementing it in the national systems, characterized by different cultures and levels of technological and administrative development.

3. The concept of antifragility

Nassim Taleb offers a new and unheard of concept of *antifragility*[13], applicable in a vast area of domains, from social sciences to security researches, economic sciences, etc. This refers to the systems' capacity to face shocks, evolving and improving after that. Antifragility is a superior concept, evolved from resilience. Resilience is about facing the shocks and coming back to the initial state, but antifragility requires growth and evolution because of the shock, of the randomness and of the incertitude. The revolutionary character of this concept set forth by Taleb is given by the solution he offers in reference to the systems' non-alignment and to their inter-dependence.

The comparison used by Taleb is more than relevant and revealing for a better understanding. If we admit that the systems are, in their vast majority, fragile, we can metaphorically resemble them to the myth of *Damocle's Sword*. The uncertainty, the danger of failure, are constant threats, the impact and the damages of which (even the collateral ones) cannot be estimated. Resilience is supposed to be a response to counter-acting the imminence of threats. The comparison would be, mythologically speaking again, with the *Phoenix Bird* who, every time it dies, is reborn from its own ashes. It is very important for a system to have the ability to recreate itself after the destabilization sustained, but it is, also, more important for it to be able to evolve and to become better, stronger and more stable. As such, the eloquent comparison would be, referring again to mythology, with the *Hydra of Lerna*. Every time when this creature's head is cut, two heads grow in its place. This, according to Taleb, represents the essence of the concept of antifragility. As such, the most desired aspects are represented by the possibility of regenerating, of improving.

3.1. Antifragility through competitive intelligence

Anticipating the evolutions and the fast transformations which appeared within the markets or the various industries, represents challenges that the companies' managers find harder and harder to deal with. Starting from certain given situations, formulating the (short, middle and long-term) strategies represents a major step on which the survival of the company itself depends.

The C.I. Analysis requires a vast procedure through which the information identified are classified according to usefulness, evaluated, analyzed and, in the end, awarded to the decision-makers as complex analyses, destined to gaining competitive advantages. Each manager's essential purpose is to gain profit (or a profit as big as possible), and this is one of the main economic indicators which signals whether the strategies chosen are favorable. Here it is important that we specify the fact that the impact made by a C.I. Analysis is not an immediate one, and that it cannot be seen immediately in the growth of the company's profit.

From the point of view of improving the quality of the products, the C.I. Procedures lead to a multitude of benefits, through the innovation they impose both on the companies as well as on the sectors and on the domains in which they operate.

CI requires two working directions: one aimed toward inside (the company's internal environment) and one aimed toward outside. If the first one aims at a deeper analysis of each separate department, with working structures, procedures, and organigrams, the latter aims at fundamentally knowing the competition. In fact, the internal analysis represents a complex

[13] Nassim Nicholas Taleb, *Antifragil. Ce avem de câștigat de pe urma dezordinii*, Curtea Veche Publishing House, Bucharest, 2019.

audit activity, which starts always from a SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) – a radiography of the company. Once made, we must try to eliminate the weak points, to remove the threats, to exploit the opportunities and to build starting from the strong points. This analysis is made on the entire company but, also, on departments, divisions or domains that are more difficult to quantify, like values and organizational culture. The internal audit requires calculating a vast number of indicators: economic, performance-related, financial, fiscal, etc., who, together with the SWOT analysis, constitute a complex and objective radiography of the company.

3.2. Competitive Intelligence as a way of working

Chris West, in his work, *Competitive Intelligence* (2001), offers a working method for CI aiming at splitting by four vast categories of information collection and analysis:

A. Who are the competitors? (Actual or future ones);

B. Profiles of the (current or future, potential) competitors;

C. Data interpretation;

D. Counter-intelligence.[14]

The collection of the information from the external environment is carried out continuously, it is a procedure which, once started, it is continuously improved and perfected, the purpose being represented by strategies, tactics who, in their turn, are active processes with a greater degree of adaptability.

Therefore, we observe that, essentially, the purpose of CI is to make it possible for a system (or a company as in our case) to not only resist shocks, the unforeseen and the provocations, but to evolve and improve itself as a result of these. The need for business intelligence-type systems can be easily explained: in order to survive on the market under the actual competitive terms, a company must try to develop a success strategy; and, in order to progress, it needs the ability to anticipate the future conditions. Understanding the past is the best way to be able to predict the future. Business intelligence does this[15].

The exclusive focus on gaining information is not enough, the ability to analyze and understand the evolution of the economic environments and to address the proper questions to the proper sources is necessary. The intelligence process' functional models, the approach to the open sources, the unaltered spread of information, require a special rigor but, also, honesty and scrupulousness. Exactly because of this complexity, the C.I. Field is a difficult one to understand, and an even more difficult one to apply. Monitoring the market flows, the emerging technologies and the law requires a continuous preoccupation. A plurivalent and complex C.I. Analysis includes the work carried out by more specialists activating in a large number of domains (marketing, public relations, financial-accounting, legal, etc.) and who have the same purpose, namely: bring value to the company they work for.

4. Antifragility – as a response to the instability of the economic environment

One of the principles of economic security starts from the premise that economic operators work more competitively in an unsafe market. The fact that, in the economic environment, we cannot talk about safety and balance, and unsafety raises competitiveness, stimulates the creative spirit, the ability to analyze and to provide, on one side. On the other hand, the fluctuations and the destabilizing events affect the economic operators in their vast majority, whatever the emerging markets.

[14] Chris West, *Competitive Intelligence*, Palgrave Publishing, 2001, pp. 222-228.

[15] Valentin P. Măzăreanu, "Inteligență în business intelligence", *Analele Științifice ale Universității* "*Ioan Cuza*" *din Iași,* 2006.

Conceptually, the economic environment can become antifragile, evolving through the fact that it was first exposed to fragility. An antifragile economic environment learns from the mistakes and benefits from fragility. The ability of knowing by trial, through the mistakes, leads to understanding the system. The items exposed to volatility, to fragility, but also to shock, disorder, risk, and incertitude become better, they adapt and evolve toward a status of antifragility. Volatility and fragility can lead both to earnings as well as to losses, but what's more important is for the disadvantages to be fewer than the advantages. For what is related to the ability to face risks, shocks, essentially, this is about knowing by trying[16] which, in the end, leads to understanding the system and to obtaining the antifragility status.

The financial crisis in Romania, which has debuted in 2008, represents a form of post-traumatic growth but, also, a form of knowing by trying, making it possible for the economic environment to be reorganized with European financial help. The economic environment can reorganize itself from the point of view of antifragility, following the building model from the 2008 crisis but, also, based on the proposals by CESE for reconstruction after the crisis caused by the COVID-19 pandemics[17], as a result of the proposals made by the European Commission with reference to the EU's recovery tool („Next Generation EU").[18] This plan aims at reorganizing the economic environment in order to sustain certain sectors (hotels, tourism, transportation, culture), small and medium enterprise systems but, also, in order to generate competitivity within the big European companies system. As such, a set of economic policies can generate the reorganization of the economic environment and obtain the antifragility status, together with macroeconomic stabilization function assured by MES[19], a set of fiscal measures beginning by temporarily adopting a set of flexible regulations in the fiscal field and in the one of state aids.

The recovery plan, valued at 750 billion Euros, within the multiannual financial framework for the 2021-2027 period, will be implemented in three steps[20]:

- The European countries' support in recovering[21] (Assistance for recovery and for cohesion, consolidated rural development programs).
- Starting the economy and support for private investments (Support tool for solvability, consolidated InvestEU program).[22]
- Learning the lessons given by the crisis[23].

Through CI we can overcompensate the economic environment's instability. The opening toward information is exclusive to the developed economies, with tradition, who can

---

[16] Matt Ridley, "Taleb on emergence and trial and error", *Wall Street Journal*, 2012, URL: http://www.rationaloptimist.com/blog/antifragility/, accessed on 29.08.2020.

[17] *Rezoluție privind „Propunerile CESE pentru reconstrucție și redresare după criza provocată de pandemia de COVID-19: UE trebuie să fie ghidată de voința de a fi o comunitate cu destin comun*, bazată pe lucrările subcomitetului „Redresare și reconstrucție după COVID-19", URL: https://www.ilegis.ro/eurolegis/ro/index/act/73599, accessed on 28.09.2020.

[18] "Recovery plan for Europe", URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe_en, accessed on 28.09.2020.

[19] *Rezoluție privind „Propunerile CESE..., op.cit.*

[20] *The EU budget powering recovery and resilience*, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe_en#theeubudgetpoweringrecoveryandresilience, accessed on 25.09.2020.

[21] *The pillars of Next Generation EU*, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe/pillars-next-generation-eu_en, accessed on 28.09.2020.

[22] *Recovery and resilience facility: helping EU countries to come out of the coronavirus crisis stronger*, European Comission, URL: https://ec.europa.eu/info/sites/info/files/2020mff_covid_recovery_factsheet.pdf, accessed on 25.09.2020.

[23] *EU budget for the future*, URL: https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/2020_rescEU_MFF_en.pdf, accessed on 25.09.2020.

understand the need for intelligence and do not attribute it exclusively to the state. Because both entities – the statal and the non-statal one (the enterprise) – share uncertainty as a characteristic that is common in their own functioning and development. As such, the need and the procedure for obtaining intelligence are similar.

According to the FBI, "the intelligence cycle is the process aimed at developing the raw data into intelligence in order to be used by the decision-makers"[24].We find out this process circular nature and the natural way in which the stages appear, as well as, sometimes, the passage to a future stage might suppose going back to a previous stage, supplying the intelligence product at the end of the cycle generating new requests for information, which will lead to restoring the intelligence process.

The first stage to identify the needs for intelligence is where the necessary information and the domains in which intelligence is expected to have a contribution for decision-makers are defined, as well as the decisions aimed at prioritizing these needs for information to assure the support aimed at developing the intelligence product that will contribute to protecting national interests.

The second stage of planning and direction is the stage aimed at organizing and coordinating the entire intelligence activity and requires action plans, from identifying the need for information to delivering the intelligence product to the beneficiaries, so as to comply with their requirements. The collection of the raw data is made based on the requirements set and these can be carried out by using one or more specific types of collection. The processing and the exploitation of the data collected requires their conversion into information, their insertion in the data base in a form that can be used in the next stage of analysis. Data conversion can be made through various methods like decrypting, translating, interpreting the data collected, etc. Within the stage aimed at analyzing and producing intelligence, the raw information, according to their certitude, validity and relevance, are subject to integration, evaluation, analysis and transformation in an intelligence product.

In the last stage of spreading and feedback, the intelligence product is supplied to the beneficiaries, and the decisions aimed at acting or restarting the intelligence cycle can be taken based on it, as a result of the appearance of new information. It is recommended that, after the intelligence product has been delivered and received, a dialog should take place between the producers and the beneficiaries of the intelligence, in order to discuss in what measure has the intelligence product satisfied the intelligence requests and in what measure are adjustments to it needed.

Intelligence is seen as the product in the light of the intelligence cycle, a document that might take various shapes, from reports to informative bulletins, notes or projects, briefings and which constitutes support for the decision-makers working for the state or the companies. We must highlight the fact that an intelligence product, whatever its appearance, must comply with six basic principles: accuracy, objectivity, usefulness, relevance, opportunity and availability. Intelligence as a product must constitute a source to take rational decisions in order to reach the strategic purposes according to the current situation and to the provisions shown within the document.

The strategic evaluation of the economic environment has become the main axis of the evolution of the forms of economic intelligence, and the information is the raw material, useful and relevant only in the conditions of correct exploitation and in safe conditions.

The future began to be seen in close connection with the ability of leaders to develop the skills appropriate to the creation and use of economic intelligence, to exhibit behaviors adapted to the requirements of the environment, aggression and customer-focused competitive

[24] Intelligence Branch, *FBI*, URL: https://www.fbi.gov/about-us/intelligence/intelligence-cycle;/, accessed on 28.09.2020.

density. The main objective was the integrated approach (including from the perspective of experts from private and academic circles) of economic intelligence, in order to implement it in national systems, characterized by different cultures and levels of technological and organizational development.

Conclusions

Antifragility, from Nassim Taleb's perspective, represents more than resistance or toughness, it is a characteristics of things to develop their ability to adapt, to be flexible and elastic. The antifragile evolves, becomes better and makes it to conceive its own defense measures, in order to adapt and to respond to shocks.[25] Those who adapt, those who carry the progress on, using rationally their resources, can benefit from the shock. This adapting can be considered as being a "post-traumatic growth". Given the fact that the world is a complex system, with non-linear reactions, the damage caused to a party, is another party's gain. This damage is much smaller than the future benefits, because it represents evolution, gain for the entire system as a whole, a "post-traumatic growth" being the result of it[26].

Evidently, the ability to adapt and to provide is not easy to be made. The companies are obliged to manage the vulnerabilities they face, to deal with challenges and to resist against threats.

As such, the most performing working method belongs to the field of CI, its mission being to create a decisional advantage for the beneficiary. CI represents one of the most important sources of knowledge structured during the decision-making process, if not the only one. CI is essential for businesses in the globalized international economic context and it should allow the description of the competitive environment, of the factors and of its elements, of the competitors, of the products, the requests for regulation, the structure of the prices and of the technologies included in this environment that might supply an alternative. After that, the anticipation of the evolution of these competitive factors, including the destructive technologies, the new competitors, etc. The verification of the measure in which these strategies' fundamental bases appear as being solid, if they were established properly and in compliance with the environment present and if they allow adjusting according to the changes appeared.

At the same time, CI should respond to those aspects related to contesting the strategy, the collection of useful information being subject to a proper evaluation and ongoing monitoring, the identification of the threats and of the vulnerabilities at the same time with the strong points and, also, of the opportunities and, then, identify whether, and if, the strategy assumed cannot be sustained any longer.

BIBLIOGRAPHY:

1. ***, "Intelligence Branch", FBI, URL: https://www.fbi.gov/about-us/intelligence/intelligence-cycle;/
2. ***, EU budget for the future, The European Commission, URL: https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/2020_rescEU_MFF_en.pdf
3. ***, Recovery and resilience facility: helping EU countries to come out of the coronavirus crisis stronger, The European Commission URL: https://ec.europa.eu/info/sites/info/files/2020mff_covid_recovery_factsheet.pdf

[25] Nassim Nicholas Taleb, *Antifragil. Ce avem de câștigat de pe urma dezordinii*, Editura Curtea Veche, București, 2019, p. 16.
[26] Nassim Nicholas Taleb, *op. cit.*, 2019, p. 53.

4. ***, Recovery plan for Europe, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe_en
5. ***, Resolution on "EESC proposals for reconstruction and recovery from the crisis caused by the COVID-19 pandemic: "The EU must be guided by the will to be a community with a common destiny", based on the work of the subcommittee "Recovery and reconstruction after COVID-19", URL: https://www.ilegis.ro/ eurolegis/ro/index/act/73599
6. ***, The EU budget powering recovery and resilience, URL: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe_en#theeubudgetpoweringrecove ryandresilience
7. ***, The pillars of Next Generation EU, https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe/pillars-next-generation-eu_en
8. DOUGLAS, Bernhardt, Competitive Intelligence. How to acquire and use corporate intelligence and counter-intelligence, FT Prentice Hall (Financial Times), 2003.
9. JOHNSON, Arik The Ethics of Competitive Intelligence, the Good, the Bad & the Gray, 2005, URL: http://www.aurorawdc.com/kb_02_ethics.pdf
10. MAZAREANU, Valentin P. "Inteligență în business intelligence', Analele Științifice ale Universității "Ioan Cuza" din Iași, 2006.
11. MOURAD, Oubrich, "L'intelligence économique. Un outil de management stratégique orienté vers le développement de nouvelles connaissances", La Revue des Sciences de Gestion, vol. 226-227, no. 4, 2007.
12. PORTER, Michael, Competition in the open economy, Harvard University Press, 1980.
13. RIDLEY, Matt, Taleb on emergence and trial and error, Wall Street Journal, 2012, URL: http://www.rationaloptimist.com/blog/antifragility/
14. SFETCU, Nicolae, Cunoaștere și Informații, Editura MultiMedia Publishing, 2019.
15. TALEB, Nassim Nicholas, Antifragil. Ce avem de câștigat de pe urma dezordinii, Editura Curtea Veche, București, 2019.
16. WEST, Chris Competitive Intelligence, Palgrave Publishing, 2001.

DESIGNING CYBERSECURITY SOLUTION USING BLOCKCHAIN TECHNOLOGY

Adriana-Meda UDROIU
National Institute for Research and Development in Informatics, Bucharest, Romania.
E-mail: meda.udroiu@rotld.ro

Abstract*: In this paper we aim to analyse the impact of Blockchain technology in the current context of cyber-security, especially in the area of smart cities and financial transactions. For this, we will first describe the current state of cyber-security and the problems it faces. Because blockchain technology only addresses part of the cyber-security matters, we will explain the response of this technology to each of the domain-specific issues. It is equally well-known that blockchain technology is the basis of many current applications (Bitcoin, Ethereum, Hyperledger Fabric). For smart cities, blockchain technology is used in designing cybersecurity for traffic control, financial transaction between organisation and authorities and so on.*

Keywords*: Blockchain technology; cybersecurity; confidentiality; bitcoin.*

Introduction

Generally, information security is described by three fundamental properties which, within a coherent security policy must be met simultaneously (Jason Andress, 2014): confidentiality, integrity and availability.

Confidentiality relates to prevention of unauthorized access to information. It is generally imposed either by communication through a secure channel, to which third parties do not have access, or by encrypting the information so that, even if the communication is intercepted, the information cannot be obtained or it can be obtained much too difficult without knowing a secret a priori.

Integrity lies in the impossibility to modify the information without the recipient noticing that the information no longer conforms to the original. By communicating through a secure channel, integrity is forced automatically, in the absence of any errors that can occur within the channel of communication. Thus, it is sufficient to check for errors, using methods such as checksum, cyclic redundancy check (CRC), Hamming code etc. In case of insecure channels, one will use information digests. A digest depends both on the information whose summary is made and on specific elements known only to the communicating parties so that, as a result of modifications, a valid digest cannot be recalculated by an attacker of the communication channel that has altered the original information.

Availability resides in securing information against Denial of Service attacks aiming to block access to it, including to those who are authorized to access it. Resistance to such attacks is carried out both by means of designing the access to information so as not to allow blocking application resources with too many requests, but also by filtering a large number of requests and limiting them to a number they can be processed. (M. Udroiu, 2010)

Cyber Security is aimed at imposing compliance with some or all of the underlying components of information security (confidentiality, integrity and availability), depending on

how necessary is each of them, in the virtual environment which subsumes all communications through an electronic channel.

Blochchain technology

Problem

The cyber security issue focuses on critical information that attackers could benefit from, such as user personal data, bank transaction data, or patient health data.

Monetary transactions are rather simple in the physical environment, because the currency of the buyer is transferred to the seller in return for a product or service. In the virtual environment, however, numerous problems arise, in particular due to the fact that it is very easy to multiply a certain piece of information, since it is represented merely by a string of bits that can be easily copied, as opposed to a physical object, whose multiplication requires knowledge about the manufacturing process, and perhaps even an investment that would make it possible to run that process. Thus, if in the virtual environment the currency would be held by each user, as it happens in the physical environment, one would very easily multiply the amount of money one holds.

This is called the double-spending problem, and usually is solved through a trusted third party that mediates transactions among customers. In this way may be viewed online banking transactions, banks being the trusted third parties who hold funds of each client and do not allow the use of the same funds in several directions. The drawback of this solution is that there is a single check point, and if this is successfully attacked, the whole system would be compromised. Also, in terms of availability, a check point is very vulnerable to DDOS (Distributed Denial of Service) attacks. A third problem with this solution based on a trusted third party that mediates the transactions is the need to entrust personal information to this party. With the spread of technology, private data protection is an issue increasingly more present, and custody of personal data of a single point of control can lead to leakage of confidential information.

Solution

Blockchain technology responds to these problems, being a distributed solution that can check all transactions securely as long as more than half of the participants in this distributed network act righteously.

This solution was originally described in an article (Satoshi Nakamoto, 200) signed by Satoshi Nakamoto and uses a peer-to-peer network in which the true result (trust) is given by the majority holding the highest calculation power. The application referred to in that article is Bitcoin, an electronic payment system using a virtual currency that is trying to simulate the real world gold, in the sense that although it has no intrinsic value, it can be obtained through an effort (mining) (https://en.bitcoin.it/wiki) and it can be used as currency exchange against products or services.

The Blockchain is a chain of blocks that contain information about all transactions made by users. If at some point a chain splitting occurs, where more competitors want to continue a chain differently, the valid variant of the chain is the longest chain variant. Thus, the system status, the valid version, the truth is determined solely by the information stored in the longest chain, because the set of validated transactions determines the State of affairs and the wealth of each user of the network.

The Blockchain is based on a peer-to-peer network in which any participant that wishes to carry out a transaction spreads a message with that transaction to all nodes on the network, or to a sufficiently large number of nodes. Thus, each node (also called a miner) will

get a number of transactions that it will group into a so-called block. Forming such a block requires fairly large computing resources, so that all nodes compete to be the first to build a new block. Also, the new block needs to follow an existing chain of blocks, so the data of the new block depends on the data in the previous block (which in turn depends on the data in the previous block, and so on). At the time when a new block is being constructed in a node, it is sent to all other nodes to be added to the chain.

In these circumstances, if the block is indeed valid, all nodes must add the new block and continue the construction of the chain following this new block. The reason the nodes do not continue to work on the block preceding the new block is that the longest chain is considered valid. Thus, if they continue to work on an old block, the chain that would end with that block would probably be the shorter, and all other nodes will regard it as invalid, so any reward received for building this block is also null.

Since the block is located at the base of the construction of a blockchain, the way it is constructed is of particular importance. Without going into details related to a specific implementation, the block contains a list of valid transactions (duly signed by the party that operates the transaction), which are grouped and one which is carried out a digest. Also, the block contains the digest corresponding to the previous block, so direct dependency between the new and the previous block can be verified.

Such information, however, would be easy to obtain, thus not meeting the condition that blocks and resources must be complex. Therefore, in order to make building new blocks more difficult, a block gets added a certain number called nonce decided so the digest of the entire block, including this number, would contain a defined number of bits from 0 to the end of the signature. The problem becomes more complex as the number of necessary zeros gets bigger. Accordingly, each node on the network will search for numbers and try to be the first one to find a number resulting in a valid block, with a signature that contains the corresponding number of initial zeros.

What this method does, apart from giving all nodes (miners) a chance related to their calculation power, is that each node has a different block for which it has to find a corresponding nonce, so a linear search would not be a disadvantage even for the slowest miners. The difference between the blocks for which the nonce is mined for consists, on the one hand, in the fact that it is possible for transactions included within the block to differ from one block to another (the transactions are submitted by using the best effort approach - not all get to all) but mainly because there is a special transaction that each miner makes it towards himself, which will change the signatures even for blocks containing the same transactions collected from the network.

A note related to building a new block is that adding a larger number of transactions does not slow down the search for a corresponding nonce, because the block's digest is made only over a digest of all the transactions.

There are two methods for rewarding the miners. On one side, each new built block brings a self-awarded reward due to the fact that the miner includes a special transaction, that doesn't have a source but is directed to the miner (or to whomever the bloc-building miner wishes). Therefore, this reward is effective only when the miner succeeds in being the first to build the block, to send it to the other miners and, by doing so, the block is included in the main chain. Thus, statistically, the number of blocks built by a miner should be proportional with the calculation power the miner uses. Also, the reward as a value determined in advance and that depends on the current block's index related to the chain's start (otherwise, each miner might reward himself to his liking). If a miner does not award himself an appropriate value, his block will not be included in the blockchain even if he was the first one to complete the block because is not being deemed valid by other miners.

The second source of income of the miners are the received transactions, which often pay a fee to the miner which will include the transaction into a valid block. The amount of these fees is up to the person making the transaction, and the bigger the amount the higher the priority that the transaction would be introduced into a block by the miners (because miners can choose which transaction to include in a block), and so, the transaction would be faster. Because the reward for each block decreases over time, this would become the main source of venue for miners.

Starting from the double-spending problem, launching an attack on a blockchain is very complex, therefore this technology is considered to be very resistant to attacks.

In order to launch such an attack, one needs to make a transaction validated by the seller, and then a new transaction on a parallel chain (it is impossible to have on the same chain two transactions using funds from the same source but different destinations), this second transaction must transfer the same funds to another seller, or to the personal wallet, and this parallel chain must be longer the original chain so that the first transaction would be invalidated (although the product or the service has been obtained because the initial transaction has been validated by the seller / provider).

If the first transaction was included in a block on the chain, there is, with enough computing power, a chance that two consecutive blocks are computed on a parallel chain before the second block is computed on the main chain. The problem is that, for the main chain the whole network is making computational efforts, while on the parallel chain participates only the attacker. If we stick to the premise that the attackers do not have more than 50% of the entire network's computational capacity, the more blocks are computed on the main chain, the time taken by the attacker to outdo this chain grows exponentially.

Thus, in order to limit the chances of success of such an attack, if the seller wants to be sure of a transaction, it must wait for a number of blocks to be added to the chain following the block containing his transaction. Generally, after three blocks have been added to the chain, information within the block are considered to be safe, since it is very difficult for the attacker to compute more than three blocks in advance compared to the main chain.

Also, in order to diminish the possibility of such attacks, a very used method is offering transaction fees that are high enough so the venue of a participant that has computational power would be comparable, in case of an attack, to the venue resulted from processing correctly a large number of blocks.

The Proof-of-Work concept refers to the proof of correctness of a result depending on how much computational power has been used. This is used currently in the Bitcoin network blockchain because the valid chain is the one that implied most effort in calculating valid blocks.

Due to the development of large computing centers, Proof-of-Work was replaced with Proof-of-stake, where participants are trusted according to the venue they have in the currency of the respective network, which brings greater protection against centralizing tendencies. Nevertheless, using this solution can lead to certain problems because it could be more efficient for a miner to vote all parallel chains that are formed instead of concentrating only on the longest chain, which is more effective in the PoW method, fact that could affect prevention of the double-spending problem (https://github.com/Ethereum). To solve this problem, two possible solutions were found.

The first one is called Slasher and penalizes users that contribute with blocks on several chains simultaneously. In case a participant of the network validates blocks from parallel chains, he/she loses the rewards for those blocks and 33% of the reward is awarded to the participant who discovered this fact. This solution has its drawbacks, because miners must connect frequently to the network, and if 25 out of the 30 miners assigned consecutively to validate blocks cooperate on an attack, it is possible they simulate a majority and carry on a

double-spending scheme. Therefore, the block validators must be well-know and trustworthy. If these risks are acceptable, then the solution is viable.

The second solution is penalizing participation to an invalid chain. This approach is somewhat similar to that of PoW, where participating in a wrong chain is the default. This approach implies greater risks to miners which unwillingly might have not mined on the winning chain when splitting occurred, but, on the long run, these risks are diminished. Thus, the advantage of this method it is that is not necessary to know the validators a priori.

Applications

The most known applications of the blockchain technology and the innovations it facilitated are: Bitcoin, the promoter of this technology, Ethereum, based on Bitcoin, but with a whole new arsenal of possibilities and Hyperledger Fabric, that changes rather significantly the approach concerning this technology.

Bitcoin (https://bitcoin.org/en/) is the promoter of the distributed crypto-currencies and has, still, the most significant presence on the capital markets (according to Coin Market Cap https://coinmarketcap.com/all/views/all/).

At the end of 2013, the inventor of Ethereum, Vitalik Buterin, advanced the idea of a sole blockchain that could entirely use the capabilities presented by all the other solutions. This blockchain would have been programmed to execute complex calculations summing the other projects. Implementation of this idea took place in 2014, with help from Vitalik Buterin, Gavin Wood and Jeffrey Wilcke. This idea was rather successful, taking into account that nowadays Ethereum is the second crypto-currency as capital share, after Bitcoin. This project is based on the Bitcoin principles, therefore, we will present only the details that show the differences between Ethereum and Bitcoin. Hyperledger Fabric is a blockchain framework and is part of the Hyperledger projects sustained by The Linux Foundation.

Differently from Bitcoin and Ethereum, which are permissionlesș which means that anybody can join the network, Hyperledger Fabric is permissioned, meaning that only certain users can join such a network. This kind of network focuses on offering the possibility to build private transactions and confidential contracts, as opposed to those from the Ethereum network, which are public.

Conclusion

Security is obtained through consensus algorithms that use methods such as Proof-of-Work, Proof-of-Stake, SIEVE and so on. These algorithms solve the double-spending problem by involving the majority of the network's users in assessing the correctness of the transactions.

Apart from the security offered by the cryptographic algorithms considered, at this moment, as being safe, this technology brings other benefits, such as high availability, low cost (because it does not involve intermediaries), higher reliability, transparency and confidence - users do not need to put their trust into an entity.

Also, with the help of intelligent contracts, complex politics may be enforced, politics that could determine transactions complying to rules clearly established a priory by network users. This technology, grace to its flexibility, offers a new range of possibilities to the electronic transactions, and the areas it can be used are limitless.

Acknowledgements: *This research work was supported by a grant on the Romanian Ministry of Innovation and Research, UEFISCDI, project number 8SOL/2018 within PNCDIII, project code: PNIII-P2-2.1-SOL-2017-09-0102, project name: Integrated Information System for Management of Activities (IISMA) (http://siima.pub.ro/en/home/)*

BIBLIOGRAPHY:

1. ***, "Anonimity", *Bitcoin wiki*, URL: https://en.bitcoin.it/wiki/Anonymity
2. ***, "Frequently asked questions", *Bitcoin wiki*, URL: https://en.bitcoin.it/ wiki/Help:FAQ
3. ***, "Script", Bitcoin wiki URL: https://en.bitcoin.it/wiki/Script
4. ANDRESS, Jason, "The basics of information security: understanding the fundamentals of InfoSec in theory and practice", Syngress, 2014.
5. BUTERIN, Vitalik, "Slasher: A punitive proof-of-stake algorithm", URL: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/
6. CLEMENT, Allen; WONG, Edmund L.; ALVISI, Lorenzo et. al., "Making byzantine fault tolerant systems tolerate byzantine faults", *NSDI*, Volume 9, 2009.
7. NAKAMOTO, Satoshi, "Bitcoin: A peer-to-peer electronic cash system", 2008.
8. NOEGEL, Scott B., "Atbash in jeremiah and its literary significance: Part 1", *Jewish Bible Quarterly*, 1996.
9. SHOR. Peter W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Review*, 1999.
10. UDROIU M., "A new approach for implementation the EU NIS directive in Romanian institutions – information security manager training program", in *The 11th International Conference on Education and New Learning Technologies, EDULEARN, 2019 Proceeding*, 2019.
11. UDROIU M., "Securitatea informațiilor în societatea informațională", Ed. Universitară, 2010.

ENVIRONMENT AND HEALTH NEXUS AS ENABLER FOR SUSTAINABLE DEVELOPMENT AND SECURITY

Luminița GHIȚĂ
Pd.D. Student, "Carol I" National Defense University, Bucharest, Romania.
E-mail: ghita.luminita@gmailcom

Abstract*: Based on the recent evolutions of international trends, environment and health issues are more than ever interlinked with security and sustainable development. The considerations of international community comprise many debates, initiatives and processes that are key drivers to bring together environment and health in the context of security and sustainable development. I present in the paper the regional process on Environment and Health under the United Nations Economic Commission for Europe, the international negotiations on adopting a resolution on Environment and Health during the Third Session of the United Nations Environment Assembly, the main sensitivities and the interlinkages with sustainable development agenda and security.*

Keywords*: environment security; pandemic; international negotiations; sustainable development goals (SDG); One Health; Environment and Health Process; United Nations Environment Assembly (UNEA); Rio+20.*

The current pandemic crisis reveals our vulnerabilities as humans, threaten by the spreading of infectious agents and enhancing of the risk of diseases. The impact on society and economy generates pressure on administration and health systems and could change our patterns of living. In spite of our major role, humans are part of the ecosystems, impacting ecosystem's components and modifying fundamental ecological processes.

The risk on human health represents a risk on human life. In this context, the health dimension and ecological dimension of security leverage the focus on considering the interlinkages between Health and Environment as relevant components of 2030 Agenda for Sustainable Development.

The world population[1] counts 7.8 billion and could reach 8.5 billion in 2030 and up to 9.7 billion in 2050. This will generate higher pressure on natural ecosystems and the increased competition for natural resources. The pressure of growing population in relation to migration related of poverty, conflicts or extreme weather events exceed the capacity support of the Earth ecosystem and generate deterioration of soil quality, water supplies, resource scarcity and irreversible phenomena such as climate change. In relations with those factors' conflicts are often exacerbate the problems. Migration is an important element of household strategies to increase or diversify sources of income.

The globalization of our society, the development of international trade and the intense travel of people around the world generated an unpreceded movement of people, animals, and animal products, intensifying the potential of the diseases to be spread quickly across borders and around the globe. These changes have led to the spread of existing or known (endemic) and *new or emerging zoonotic diseases*, which are diseases that can spread between animals

[1] ***, "Population Division World Population Prospects 2019", *UN*, URL: https://population.un.org/wpp/Download/Standard/Population/, accessed on 23 August 2020.

and people. Examples of zoonotic diseases include: Rabies, Salmonella infection, West Nile virus infection, Q Fever (Coxiella burnetii), Anthrax, Brucellosis, Lyme disease, Ringworm, Ebola and most recently Covid-19.

The report[2] "Global Trends 2030: Alternative Worlds" published by US National Intelligence Council (NIC) in December 2012, aiming to "stimulate thinking about the rapid and vast geopolitical changes characterizing the world today and possible global trajectories during the next 15-20 years", presented that one of the potentials "black swans" that could cause one of the greatest disruptive impact at global level is *severe pandemic*. The report cannot make the prediction of the *specific pathogen which will be the next to start spreading to humans,* or when *or where such a development will occur* "but humans will continue to be vulnerable to pandemics, most of which will probably originate in animals". It is underlined that "an easily transmissible novel respiratory pathogen that kills or incapacitates more than one percent of its victims is among *the most disruptive events possible*. "*Such an outbreak could result in millions of people* suffering and dying in every corner of the world in less than six months."

More recently, in 2018, The World Health Organization (WHO) predicted the "*Disease X*" in a report[3] as the outcome of consultations held in Geneva (6-7 February 2020) – "the 2018 Annual review of diseases prioritized under the Research and Development Blueprint" (WHO R&D Blueprint). In elaboration of the WHO R&D Blueprint contributed experts in: microbiology of severe diseases, including virology, bacteriology and mycology; clinical management of severe infections; epidemiology, in particular during health emergencies; public health policy, including emergency response; animal health, including veterinarians expert in zoonoses from both livestock and wildlife; and anthropologists; as well as experts from defense or security sectors familiar with biological weapons. These experts made use of a tailored prioritization methodology developed and validated by WHO.

The consultation aims to reduce the time between declaration of a public health emergency and the availability of effective diagnostic tests, vaccines, antivirals and other treatments that can save lives and avert a public health crisis. The report calls for an urgent need for *accelerated research and development for*: Crimean-Congo Hemorrhagic Fever (CCHF), Ebola Viral Disease and Marburg Viral Disease, Lassa Fever, Middle East respiratory syndrome coronavirus (MERS-CoV) and Severe Acute Respiratory Syndrome (SARS), Nipah and henipaviral diseases, Rift Valley Fever (RVF), Zika disease and *Disease X*. WHO mentioned that the order of diseases on this list does not denote any ranking of priority. Nowadays some scholars consider the Covid-19 represents the Disease X.

1. "One health" approach

The Center for Control Disease and Prevention[4] (CDC) represents a national public institute in United States of America founded in 1946 from the Program of World War II Malaria Control in War Areas of the Office of National Defense Malaria Control Activities, as a new branch of the United States Public Health Services. Due to biological warfare concerns arising from the Korean War, in 1951 was established the Epidemic Intelligence Service (EIS) with centers in many countries based on the CDC experience. The CDC expanded their areas of interests on public health including all communicable diseases and to provide practical help

[2] ***, "Global Trends", National Intelligence Council, *Director of National Intelligence*, URL: www.dni.gov/nic/globaltrends, accessed on 8 July 2020.
[3] ***, "R&D Blueprint", *WHO*, URL: http://www.who.int/csr/research-and-development/en/, accessed on 4 May 2020.
[4] ***, "One Health", URL: https://www.cdc.gov/onehealth/index.html, accessed on 8 July 2020.

to state health departments and became the National Communicable Disease Center (NCDC) in 1967 and with the addition of *prevention - The Center for Control Disease and Prevention* (CDC) in 1992. CDC is one of the major operating components of the Department of Health and Human Services and is recognized as the *US premiere health promotion, prevention, and preparedness agency.* CDC plays a central role in organizing the conferences "One Health" engaged cross-sectoral multi-stakeholders in the field of human, animal, plant health, environmentalists etc.

The first One Health Summit held in Davos, Switzerland, 19-22 February 2012, introduced the concept of "One Health" to manage health threats focusing on food safety and security. The outcome of the summit was the adoption of the Davos One Health Action Plan on the improving the public health through multi-sectoral and multi-stakeholder cooperation. In 2013, the Second International One Health Congress encouraged collaboration across disciplines to promote effective policy development related to human, animal, and environmental health.

The areas of work in which One Health approach is particularly relevant include food safety, the control of zoonoses (diseases that can spread between animals and humans, such as flu, rabies and Rift Valley Fever), and combatting antibiotic resistance (when bacteria change after being exposed to antibiotics and become more difficult to treat). The One Health Initiative represents a collaborative, multisectoral, and transdisciplinary approach—working at the local, regional, national, and global levels—with the goal of achieving optimal health outcomes recognizing the interconnection between people, animals, plants, and their shared environment.

"One Health" is an approach that recognizes that the *health of people is closely connected to the health of animals and our shared environment.* In the recent years, many factors have changed with the interactions between people, animals, plants, and our environment, the main causes being the significant restriction of wildlife habitats and the concept of "One Health" has become more important.

Human populations are growing and expanding into new geographic areas. As a result, more people live in close contact with wild and domestic animals, both livestock and pets. Animals play an important role in our lives, whether for food, fiber, livelihoods, travel, sport, education, or companionship. Close contact with animals and their environments provides more opportunities for diseases to pass between animals and people. The changes in climate and land use, such as deforestation and intensive farming practices cause disruptions in environmental conditions and habitats can provide new opportunities for diseases to pass to animals.

The World Health Organization (WHO)[5] recognizes the concept of One Health as an approach to designing and implementing programmes, policies, legislation and research in which multiple sectors communicate and work together to achieve better public health outcomes.

On the ongoing preparation for the Fifth Session of the United Nations Environment Assembly (February 2021) the debates at EU level emphasize that it is essential to integrate the "One Health" approach in regards to Healthy Ecosystems. Furthermore, a link should be made between food systems and emergence on zoonotic diseases, recognizing that most of the causes behind their emergence are primarily linked to food systems and stressing the need to enhance the transition towards more sustainable food systems, making food systems fair, healthy, environmentally friendly, economically viable and more resilient to crises.

[5] *WHO*, URL: https://www.who.int/, accessed on 9 July 2020.

2. Health and sustainable development

The 2030 Agenda for Sustainable Development and its 17 Sustainable Development Goals (and 169 target) was adopted by the United Nations General Assembly in 2015 - the Resolution A/Res/70/1. The interlinked nature of the 17SDGs and 169 targets of the 2030 Agenda represents the vehicle to tackle environment, social and economic objectives in a holistic approach, one SDG is dedicated to Health - SDG3 "Ensure health and wellbeing for all at all ages" but many SDG and targets deal with health issues. We present he main interlinkages of the others 16 SDGs with SDG3 "Ensure health and wellbeing for all at all ages" elaborated by WHO[6] as follows:

- SDG1" End poverty in all its forms everywhere" – *Prioritizing the health needs for the poor,*
- SDG2 "End hunger, achieve food security and improved nutrition and promote sustainable agriculture" – *Addressing the causes and consequences of all forms of malnutrion,*
- SDG4 "Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all" – *Supporting high-quality education for all to improve health and health equity*,
- SDG5 "Achieve gender equality and empower all women and girls – *Fighting gender inequities, including violence against women and girls*,
- SDG6 "Ensure availability and sustainable management of water and sanitation for all" – *Preventing disease through safe water and sanitation for all*,
- SDG7 "Ensure access to affordable, reliable, sustainable and modern energy for all" – *Promoting sustainable energy for healthy homes and lives*,
- SDG8 "Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all" – *Promote health employment as a driver of inclusive economic growth,*
- SDG9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation" – *Promoting national Research and Development Capacity and manufacturing of affordable essential medical products*,
- SDG 10 "Reduce inequality within and among countries" – *Ensuring equitable access to health services through universal health coverage based on stronger primary care*,
- SDG11 "Make cities and human settlements inclusive, safe, resilient and sustainable" – *Fostering healthy cities through urban planning for cleaner air and safer and more active living,*
- SDG 12 "Ensure sustainable consumption and production patterns" – *Promoting responsible consumption of medicines to combat antibiotic resistance*,
- SDG 13 "Take urgent action to combat climate change and its impacts" – *Protecting health from climate risks, and promoting health through low-carbon development,*
- SDG14 "Conserve and sustainably use the oceans, seas and marine resources for sustainable development" – *Supporting the restoration of fish stocks to improve safe and diversified healthy diets*,
- SDG15 "Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss" – *Promoting health and preventing diseases through healthy natural environment,*
- SDG16 "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at

[6] *WHO*, URL: https://www.euro.who.int/__data/assets/pdf_file/0007/319804/banner-health-SDG-era.pdf?ua=1, accessed on 10 July 2020.

all levels" – *Empowering strong local institutions to develop, implement, monitor and account for ambitious national SDG responses*,

- SDG17 "Strengthen the means of implementation and revitalize the Global Partnership for Sustainable Development" – *Mobilizing partners to monitor and attain the health-related SDGs*.

There is need of a cross-cutting approach and preventive approach to health and well-being issues to contribute to the SDGs synergistically.

In our opinion *the elements* mentioned in the highlighted (italic) text could considered as key components of a strategic plan on addressing health issues for elaborate and implement public policies on health.

3. The health and environment nexus as outcome of UNEA

The United Nations Environment Assembly (UNEA) was established based on the outcome[7] (Resolution of United Nations General Assembly A/RES/66/288, entitled "The Future We Want") of the United Nations Conference on Sustainable Development (Rio+20) held in June 2020, part of the second theme of the Rio+20 conference - *strengthening the institutional framework for sustainable development*.

UNEA represents the governing body of the United Nations Environment Programme (UNEP) and has universal participation, all UN member states are part of the negotiations process accordingly with the UNEP mandate of strengthen the environmental dimension of sustainable development. UNEA is the main international body on environmental policy at global level, convenes in sessions held at the UNEP headquarters in Nairobi to adopt decisions and resolutions on environmental matters (ecosystems management, waste and chemicals, education for sustainable development) and on the interlinkages between environment and other relevant sectors such as health, security (environment in conflict areas), sustainable consumption and production, sustainable infrastructure, mining

World Health Organization (WHO) reports that 12.6 million deaths globally[8], representing 23% of all deaths, were attributable to the environment in 2012. In children under five, up to 26% of all deaths could be prevented, if environmental risks were removed. There is the urgent need for coherent and comprehensive action towards reducing the adverse impacts of pollution to health and well-being.

On the margins of the Second Session of the United Nations Environment Assembly in 2016 (UNEA2), took place a debate on the Health and Environment nexus and UNEP produced a dedicated report "Healthy environment, healthy people", including a list of possible actions but no agreed text and no action were taken upon the debate and the report.

Based on the UNEP's mandate on the health-environment nexus, the international community urged UNEP to work in close cooperation with WHO and other relevant actors, while avoiding unnecessary duplication. It would provide an appropriate response to the resolutions related to health and the environment adopted in 2015 and 2016 by the World Health Assembly, and make sure that the environmental sector also provides its expertise.

The nexus of Environment and Health represents a strategic umbrella to streamline the way many pollution sub-topics (e.g. lead in paint, chemical and waste management, urban pollution etc.) could be integrated for a cross-cutting approach to pollution. We would also

[7] ***, "The Future We Want. Outcome document of the UN Conference on Sustainable Development 20-22 June, Rio de Janeiro", *United Nations*, New York, 2012.
[8] ***, "United Nations Environment Programme (2016). Healthy Environment, Healthy People Thematic Report - Ministerial Policy Review Session" – Second Session of the United Nations Environment Assembly of the United Nations Environment Programme, Nairobi, 23-27 May 2016.

like to underline in relation to the nexus that sustainable consumption and production, circular economy, Green Economy and similar approaches provide cross-cutting and preventive solutions to tackle pollution and thereby improve synergistically health and the environment. In more particular, we could touch upon the issues of pollution and health:

- Air, water, marine, soil pollution, impacts to health;
- The need to monitor, have scientific data and a global transboundary view;
- Most impacted groups of society;
- Awareness;
- Local prevention and action plans;
- A global agreement and goal for pollution reduction.

More specifically that it is important to tackle specific issues such as chemicals and waste, in particular pesticides and endocrine disrupters, the environmental drivers and management options to deal with antimicrobial resistance, sound (noise) pollution, the potential and benefits for health and well-being of protecting and restoring ecosystems.

On the preparation processes of the 3th Session of the United Nations Environmental Assembly (UNEA3) in 2017 the European Union and its Member States submitted a proposal for a resolution on Environment and Health. The EU and its Member States consider *that health and environment are inextricably linked* and that advancing the environmental agenda means addressing the health agenda. In the same process, Philippine submitted one proposal intitled "Strengthening health and environmental action in Asia and the Pacific and supporting the initiatives of the Asia-Pacific regional forum on health and environment". In the process of intergovernmental negotiations those 2 proposals merged in one single resolution adopted by UNEA3, document number UNEP/EA.3/Res.4 entitled "Environment and Health". The resolution was negotiated during many days and the consensus was agreed on the basis of the important outcomes of the Conferences of the Parties in the field of environment including references of the interlinkages between health and environment issues such as:

- the role of the Basel, Rotterdam, Stockholm and Minamata Conventions and the Strategic Approach to International Chemicals Management to support pollution prevention and to protect environment and health;
- the decision of the Convention on Biological Diversity (CBD/ COP/DEC/XIII/6) on the linkages between health and biodiversity;
- the work of the Intergovernmental Platform on Biodiversity and Ecosystem Services to access the health of world's biodiversity through thematic, regional and global assessments;
- the burden of disease from *environmental risks,* which according to estimates from WHO[9] amounts to *23% of total global deaths,* and the associated costs to society;
- the findings pf the Lancet Commission on pollution and health that *health effects of pollution are underestimated in existing calculations of the global burden of disease and that pollution*, which was responsible for an estimated 9 million premature deaths in 2015 - the largest environmental cause of disease and premature deaths in the world, and causes welfare losses amounting to 6.2% of global economic output; and concerned that deaths associated with ambient air, chemical and soil pollution are rising[10] ;
- the work of regional processes of health and environment (the Asia Pacific Regional Forum on Health and Environment, the European Environment and Health Ministerial process, the African Inter-ministerial Conference on Environment and Health, the joint sessions of the Arab Ministerial councils on the environment and on health, and the Forum of

[9] ***, *WHO report*, "Preventing disease through healthy environments: a global assessment of the burden of disease from environmental risks", 201), p. 86.
[10] Landrigan, Philip J. et al., "The Lancet Commission on pollution and health.", *The Lancet*, 2017.

Ministers of Environment of Latin America and the Caribbean) in contributing to the regional and national policy actions and in strengthening the environment governance around the Environment and Health nexus;

The international community agreed to affirms the strong inter-linkages between Environment and Health, including health inequalities and encourages Member States and stakeholders to continue engaging in the work of ongoing intergovernmental regional processes on health and environment in addressing the health and environment nexus to spearhead the achievement of Sustainable Development Goals of the 2030 Agenda for Sustainable Development.

On Climate and Health related issues, the Action Agenda on Health and Climate Change was adopted as an outcome of the Second World Conference organized by WHO on Health and Climate (Paris, July 2016).

The burden of disease attributable to the environment is high and persistent, and amounts to 13 million deaths each year (one quarter of all deaths), and further health concerns are posed by global challenges such as climate change and rapid urbanization. To respond to that situation, a new global strategy on health, environment and climate change has been developed and broadly supported by countries during the 72nd World Health Assembly in May 2019. WHO Global Strategy on Health, Environment and Climate change entitled "The transformation needed to improve lives and well-being sustainably through healthy environments" (A72/15). It aims at transforming the way we tackle environmental risks to health by accounting for health in all policies and scaling up disease prevention and health promotion. The strategy provides a vision and way forward on how the world and its health community need to respond to environmental health risks and challenges until 2030, and to ensure safe, enabling and equitable environments for health by transforming our way of living, working, producing, consuming and governing.

4. The European environment and health process

The environment is a major determinant of health, estimated to account for almost 20% of all deaths in the WHO European region. Concerned about the growing evidence of the impact of hazardous environments on human health, WHO Europe initiated in 1989 the first ever *environment and health process*, towards a broad primary prevention public health approach, and to facilitate intersectoral policy-making.

The European Environment and Health Process (EEHP) was aimed to eliminate the most significant environmental threats to human health and to facilitate a breakthrough for a sustainable environment and healthy -friendly societal development. The conferences are considered unique, bringing together different sectors to shape European policies and actions on environment and health.

The EEHP is coordinated and driven forward by the WHO and Environment and Health Task Force (EHTF) of the Ministers of Environment and Ministers of Health of the 53 WHO Europe Member States.

The first conference on EEHP was held in Frankfurt in 1989, followed by Helsinki in 1994 and London in 1999. In London was adopted the Charter on Transport, Health and Environment. In 2004 in Budapest was adopted the Children's Environment and Health Action Plan for Europe. The Fifth Conference was held in Parma, Italy, on 10-12 March 2010. The first political adopted outcome of the EEHP is "The Parma Declaration". Governments of the 53 European Member States set clear-cut targets to reduce the adverse health impact of environmental threats in the next decade.

The Sixth Ministerial Conference on Environment and Health took place in Ostrava, Czech Republic, 13-15 June 2017. The Ostrava Declaration summarizes the priorities in this area in the WHO European Region, provides tools to Member States to develop national portfolios for action, which they committed to develop by the end of 2018 and introduces new institutional arrangements for the European Environment and Health Process that should come into force in 2018. At this Conference, the Member States committed to develop national portfolios for action that should address the need to accelerate progress on Health and Environment and, in particular, addressing the Environment-related Health SDGs and targets of the 2030 Agenda for Sustainable Development.

The EEHP is an intersectoral process and platform for the development and implementation of policies and activities to improve environment, health and well-being in the WHO European Region. It supports and acts in synergy with regional and global policy processes:

- 2030 Agenda for Sustainable Development and Global Action Plan for Healthy Lives and Well-being for All, in which health and well-being linked to environmental and work-related factors are outcomes, determinants and enablers of sustainable development. Working through the EEHP, Member States can make sustained progress in accelerating health achievements of the number of targets of the Sustainable Development Goals (SDGs);
- Health 2020, the European policy framework and strategy for health and well-being, to which Member States committed to ensure development and implementation of coherent multisectoral strategies that emphasize system-wide and equitable preventive policies to improve environmental health conditions;
- WHO 13th General Programme of Work 2019−2023 (GPW13) addresses five platforms and eight health outcomes. Platforms 2 and 5 are related to non-communicable diseases and the health impacts of climate change, environmental risks and other determinants of health and are important areas of work of EEHP. GPW13 also calls on WHO to strengthen its normative work.

The European Environment Health Process plays a strong and visible role in the normative work of the WHO Regional Office for Europe and globally through its work on the environment and health governance.

Conclusions

In the recent years, the international community developed many initiatives and actions at global level aimed to address on an integrated approach the Health and Environment issues. We consider that the “One Health” initiative in relation with 2030 Agenda for Sustainable Development and its 17 SDGs represents a *broaden approach on targeting specific actions on ensuring health of humans and environment*. This broaden approach requires to strengthen the institutional framework on Health and Environment at global, regional, national and subnational level.

On developing health public policies, we should take into consideration the precautionary principle when scientific evidence is inconclusive and there is a substantial environmental risk to human and ecosystem health. There is a need to stress the impact of pollution on biodiversity, promote the “One health” approach and Ecosystem/nature-based solutions.

There is also a need to underline that existing science, technology, knowhow and action plans settle a strong basis to work on the policy dimension, and at the same time a necessary effort is still needed on research programs. We consider that there is a need for develop sustainable food systems to avoid the occurrence of new zoonotic diseases.

We consider that the emerging pathogens continue to represent a serious threat to human health at global level. There is a continuous need for setting of a regulatory assessment to find solutions on an inter-sectoral and integrated approach, linking Health and Environment as parts of the life-system.

The findings of the Health and Environment sciences should be considered in the holistic approach of the survival of humans among the complex mega-system of the Earth, respecting the capacity of Earth ecosystem on sustaining all forms of life.

There is a call for the development of global, regional and national strategies to tackle the environment-health nexus, including the development of adequate communication and education strategies to raise awareness on environmental and health risks and exposure. We also want to stress the importance of partnerships and inclusive governance for effective implementation of environment and health cross-sector policies.

BIBLIOGRAPHY:

1. ***, "The Future We Want. Outcome document of the UN Conference on Sustainable Development 20-22 June, Rio de Janeiro", published by *United Nations*, New York, 2012.
2. ***, "Transforming our World. The 2030 Agenda for Sustainable Development", *UN press*, New York, 2015.
3. ***, *United Nations Environment Programme Report*, "Healthy Environment, Healthy People Thematic Report – Ministerial Policy Review Session" – Second Session of the United Nations Environment Assembly of the United Nations Environment, 2016.
4. ***, *World Health Organization Report*, "Preventing disease through healthy environments: a global assessment of the burden of disease from environmental risks", 2016.
5. CHALECKI, Elisabeth L., "Environmental security. A guide to the issues", ABC-CLIO LLC, Santa Barbra, California, 2013.
6. DANNREUTHER, Roland, "The international security. The contemporary agenda", Polity Press, Cambridge, 2013.
7. LANDRIGAN, Philip J. et al., "The Lancet Commission on pollution and health", The Lancet, 2017.
8. STUGREN, Bogdan, "Ecologie teoretică", Editura Sarmis, Cluj-Napoca 1994.
9. *United Nations Report*, "World Population Prospects 2019. Highlights", *United Nations*, New York, 2019.

Websites:

www.dni.gov/nic/globaltrends
http://www.who.int/csr/research-and-development/en/
https://www.cdc.gov/onehealth/index.html
https://www.who.int/
https://www.euro.who.int/__data/assets/pdf_file/0007/319804/banner-health-SDG-era.pdf?ua=1
https://wedocs.unep.org/bitstream/handle/20.500.11822/31019/k1800154.english.pdf?sequence=3&isAllowed=y
https://population.un.org/wpp/Download/Standard/Population/

THE EVALUATION AND DETECTION OF "A MAN IN THE MIDDLE" CYBERATTACKS

Adriana-Meda UDROIU
National Institute for Research and Development in Informatics,
Bucharest, Romania. E-mail: meda.udroiu@rotld.ro

Mihail DUMITRACHE
National Institute for Research and Development in Informatics,
Bucharest, Romania. E-mail: mihaildu@rotld.ro

Abstract*: How common is a "man-in-the-middle" type of attack in the wild today and how can it be detected and prevented? What is the security impact of HTTPS interception given that more and more organizations and antivirus products intercept and inspect traffic? This paper aims to provide an answer to these questions by presenting results and conclusions of the study conducted to detect man-in-the-middle attacks on a number of popular internet websites.*

Keywords: *TLS; certificates; HTTPS; "man-in-the-middle attack"; interception.*

Introduction

Transport Layer Security (TLS) protocol in conjunction with Public Key Infrastructure (PKI) secures a significant part of today's Internet traffic therefore trust in TLS and the PKI are fundamental parts of the Web. A TLS man-in-the-middle attack is characterized by use of forged certificates to intercept encrypted connections between clients and servers. "In cryptography and computer security, a *man-in-the-middle attack* (*MITM*) is an *attack* where communication between two parties who believe they are directly communicating with each other is intercepted, relayed and possibly altered by an attacker"[1].

Hypertext transfer protocol secure (HTTPS) relies on a group of pre-trusted certificate authorities (CAs) for party authentication. However, this authentication architecture can be completely compromised in case any one of the trusted certificate authorities has been compromised.

Notary-based systems and pre-shared secrets have been proposed in an attempt to mitigate this critical flaw but these state-of-the-art techniques can unfortunately neither provide maximal protection nor resist potential man-in-the-middle attack variants.

At the other end a trust on first use technique called HTTP public key pinning (HPKP) was introduced in order to reduce the risk of man-in-the-middle attacks by associating a specific cryptographic public key with a certain web server. However, although security is increased by this feature, it cannot completely prevent attacks and has some drawbacks. For instance, "Firefox and Chrome disable pin validation for pinned hosts whose validated certificate chain terminates at a user-defined trust anchor rather than a built-in trust anchor.

[1] ***, "Robotic Process Automation", *fakecineaste*, URL: https://fakecineaste.blogspot.com/2019/09/, accessed on 28.09.2020.

This means that for users who imported custom root certificates all pinning violations are ignored"[2].

1. Evaluation

There are multiple known possible cases when an attacker is mistakenly authenticated as the server and most of them have already been seen in reality:

- Stealing the server's private key and using it along with server's valid certificate
- Stealing the CA's private key and using it to sign another certificate for the server
- Getting one of the reputable CA's to sign (either by cooperating, tricking or hacking the CA) a new server certificate
- Installing a new trusted CA on the client side (by fooling the user or hacking the client) then creating a new certificate for the server without needing any of the trusted CAs
- Using a self-signed server certificate counting on the fact that user will ignore the security warning (study [1] showed 90% of the forged certificates chains have a depth of 1 – only the self-signed server certificate)
- Exploiting vulnerabilities in the client software like the Apple "goto fail" bug [5]
- Weakened connection security due to use of poorly configured or misconfigured IDS/IPS appliances and antivirus software (62% of the traffic that traverses a network middlebox has been found to have reduced security [2]).

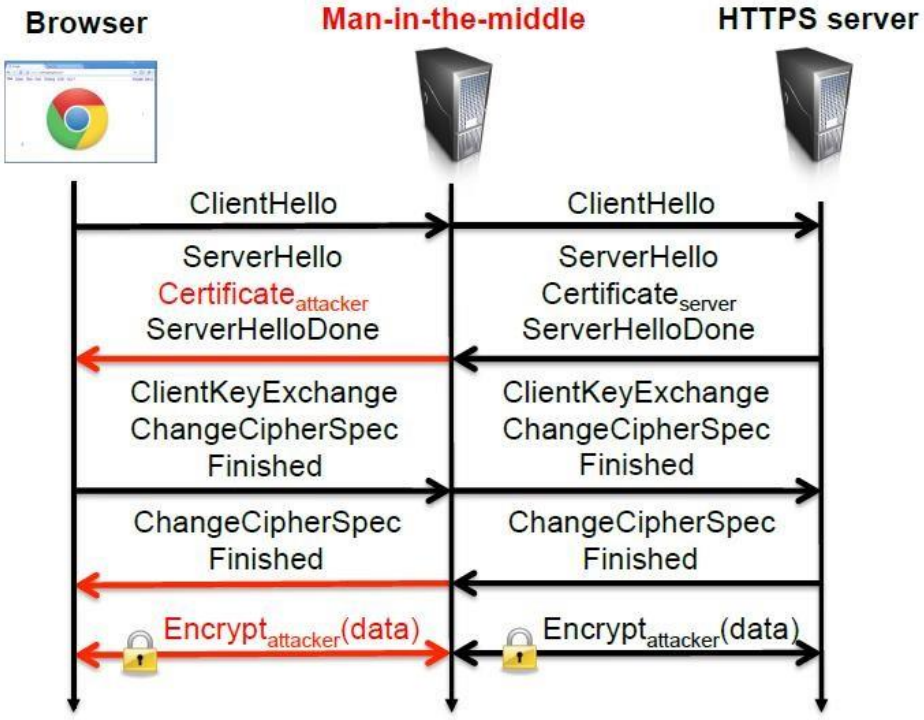


Figure no.1: Man-in-the-middle attack

Nowadays HTTPS interception done using antivirus software or corporate middleboxes has become startlingly widespread and with rightfully worrying consequences. A study [2] conducted throughout the course of 2016 revealed that between 4% and 11% percent of the traffic monitored was potentially tampered with. Current objective of my

[2] *Ibidem*.

research is to assess whether anything had improved in terms of security throughout the past two years after the awareness raised by researchers upon disclosure of the worrying results in their study [2].

Also, with the recent approval of TLS 1.3 protocol by IETF after not less than 28 iterations, it will be very interesting to learn to which extent TLS 1.3 is being incorporated and most importantly used equally by browsers, antivirus software and IDS/IPS appliances.

2. Methodology

It is well known that with each request browsers send the User-Agent HTTP header in a standardized format which can be used to identify the client browser and operating system. Although agent spoofing is possible it is highly unlikely that users spoof their own User-Agent header at a large scale as shown by Eckersley in his study [6].

In conjunction with this header each browser advertises a specific set of parameters such as supported ciphers, algorithms, extensions, etc. during initial TLS handshake, which can be used to fingerprint TLS implementation and eventually identify the client (browser).

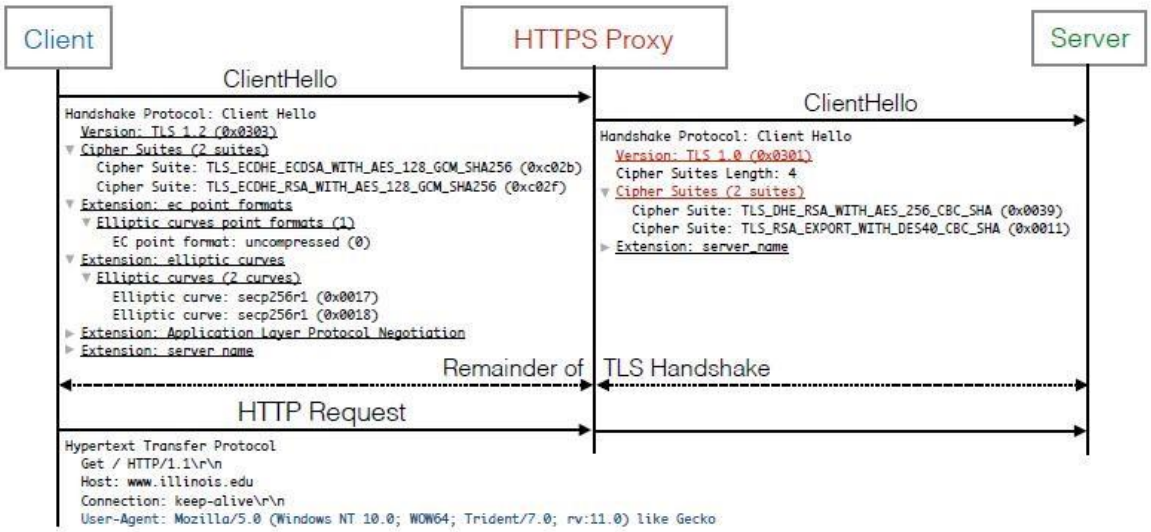


Figure no. 2: Example of HTTPS interception

The four most popular browsers – Chrome, Firefox, Internet Explorer and Safari – select unique sets of options with small variations based on their version, operating system as well as user preference. Furthermore, all these parameters are different from those used by both common libraries such as OpenSSL and popular interception middleboxes [2].

While Chrome and Internet Explorer support reordering or disabling of cipher suites Firefox and Safari have the cipher order predetermined and hardcoded which makes them easier to fingerprint due to the fact that the handshake does not vary much for different versions and operating systems. In the case of Chrome and Internet Explorer the degree of customization users or administrators are allowed to perform makes it more difficult to be certain that the fingerprint belongs to a specific browser version. For this reason, checking for instance for other unique identifiers such as the OCSP status request extension used before the supported groups extension only by Microsoft's proprietary TLS implementation – Schannel – can uniquely identify versions of the Internet Explorer browser family.

Proposed approach during the research is to analyze rather whether the specific handshake established with the server could have been generated by a specific browser than to

put together every possible combination of operating system and browser version and compare advertised parameters with those from the handshake.

Just like browsers, corporate middleboxes or security products generate specific fingerprints that are completely different from those produced by browsers. Even though almost none of these security products advertise their name or the manufacturer during the handshake, sending mismatched parameters from any of the fingerprinted browsers is a red flag indicating that the connection has been tampered with.

Some popular antivirus and anti-malware software [7] actively intercept TLS connection by injecting a new client side root certificate and subsequently generating server certificates on the fly. These products generate yet another set of fingerprints, different from the browsers, and play an active role in connection security. Whether they are beneficial or harmful, increase or decrease the level of security is a question that will be answered later on, during the research phase.

Next steps to be taken are the actual fingerprinting of different clients and build of the database containing identified TLS handshakes. The database will be used as a baseline for comparison of handshakes obtained in the wild against known fingerprints and will allow us to determine to which extent handshakes are consistent with the advertised client and eventually measure the amount of interception.

In order to quantify interception rates in the wild the algorithm to capture handshakes and to compare known fingerprints against those of incoming connections would have to be deployed server side at the border of one or more globally or widely used websites. Another option which requires fewer resources would be to simply agree with the partners that they will collect a large enough number of handshakes on their servers and later on provide us with gathered data in order to perform the analysis offline.

Entering into a thesis partnership with one or more companies hosting reputable websites visited by a large number of people is of paramount importance to be able to conduct the research. Together with technical activities main focus will be put on finding partners interested and willing to cooperate in this endeavour.

BIBLIOGRAPHY:

1. ***, "Robotic Process Automation", fakecineaste, URL: https://fakecineaste.blogspot.com/2019/09/
2. ***, *OPSWAT*, "Windows Anti-malware Market Share Report", URL: https://metadefender.opswat.com/reports/antimalware-market-share#!/
3. DUCKLIN, Paul, "Anatomy of a "goto fail" – Apple's SSL bug explained, plus an unofficial patch for OS X!", Sophos, URL: https://nakedsecurity.sophos.com/2014/ 02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explainedplus-an-unofficial-patch
4. DURUMERIC, Zakir; MA, Zane; SPRINGALL, Drew et. al., "The Security Impact of HTTPS Interception", URL: https://jhalderm.com/pub/papers/interception-ndss17.pdf
5. ECKERSLEY, Peter, "How unique is your web browser? In Symposium on Privacy Enhancing Technologies", 2010, URL: https://panopticlick.eff.org/static/browser-uniqueness.pdf
6. HUANG, Lin-Shung; RICEY, Alex; ELLINGSENY, Erling and JACKSON, Collin, "Analyzing Forged SSL Certificates in the Wild", *Carnegie Mellon University*, URL: https://www.linshunghuang.com/papers/mitm.pdf
7. MATTSSON, John; NÄSLUND, Mats, "Research, Detection and Mitigation of HTTPS Man in the Middles and Impersonators", URL: https://www.w3.org/2012/ webcrypto/webcrypto-nextworkshop/papers/webcrypto2014_submission_19.pdf
8. YABING, Liu; WILL, Tome; LIANG, Zhang, "An End-to-End Measurement of Certificate Revocation in the Web's PKI" URL: https://mislove.org/ publications/SSLClient-IMC.pdf

THE INFLUENCE OF POPULISM IN UNDERSTANDING THE CONCEPT OF SECURITY

Dorin Alin GAL
Ph.D. Student, "Carol I" National Defence University, Bucharest, Romania.
E-mail: doringal07@gmail.com

Abstract: *With populism becoming one of the buzzwords that characterize international relations today, its ideas stand to influence the way leaders and actors woldwide now understand the meaning of security. Since this is a term with an exceptional ability to transcend traditional ideological lines, it has the potential to cause an impact regardless of the space where it is being used and, as a result, is able to have an impact through modern-day populist leaders regardless of their original affiliation. By stating a working definition of populism as we understand it right now and also of the traditional concept of security, we stand to analyze the way in which security issues and any subsequent decisions made are being influenced under this new context that we find ourselves in today.*

Keywords: *populism; security; volatility; anti-elitism; anti-pluralism.*

1. Populism: a gradual evolution

In order to be able to fully develop the ideas of this paper, we find it important, due to the flexibility of the term "populism" to first settle exactly what perspective we are going to use when talking about it. If we look at the generally accepted definition, it can be defined as a set of ideas whose two main elements, found in all of its manifestations, are anti-elitism and anti-pluralism[1]. During recent times, the lack of extended research on the topic as well as populism's own rise due to some effects of globalization have influenced leaders characterized as "populists" to also be studied as a group in order to try to determine the characteristics of this ideology, and not just individually with the use of the information which is already available regarding populism. As a result, descriptive methods of research, particularly the ones focused on group interactions and relationships, represent a more than adequate way of studying the effects of this ideology. Using observation and document researching we will be able to pinpoint the challenges offered by populism, challenges that come from the present-day status quo.

Four years ago, the European Union's then-Foreign Policy chief, Federica Mogherini, hosted a meeting of the European bloc's then-28 Foreign Ministers in order to talk about the collective reaction to Donald Trump becoming the 45th President of the United States of America. The objectives of this meeting were inherently good and standard practice when it comes to the EU's general objectives: get the European parties to collaborate and initialize a plan to salvage the two great collective achievements past-World War II: the Euro-Atlantic relationship, firmly anchored to this day by NATO and everything that it stands for, and the USA's commitment to Europe's security and values. Instead, the actors that were present there failed to see the need for a general consensus and got side-tracked by personal

[1] Johannes Plagemann, Sandra Destradi, ,,Populism and Foreign Policy: The Case of India", in *Foreign Policy Analysis*, 283, 2019, URL: https://doi.org/10.1093/fpa/ory010, accessed on December 27, 2019.

differences. The leaders of the continent were unable to reach common ground in terms of measures that were required to develop Europe's defensive potential. Also, they did not perceive the degree to which the changes in the United States were going to influence the global security environment and the balance of the transatlantic relationship[2]. While the meeting was intended to be a framework for the way in which European states would contribute to NATO's budget and the entire multilateral structure going forward, this reaction also shows the way populism can influence even those in power, willingly or not.

What the world only gradually began to understand in the years that followed was that the new American president was not, by himself, the reason for the new form of instability caused by people losing their faith in governments but was, and is, its greatest manifestation. Populism was not perceived as a threat when it first started and only during the first decade of the 2000s did political actors start taking it more seriously and more studies started to emerge. However, these were still focused strongly on empirical data and on finding out the reason behind why some actors were becoming increasingly successful using this ideology. Almost none of them, however, took the time to investigate into what this could mean for the future, especially regarding the shifting in people's beliefs and why they were suddenly turning towards authoritarian-like leaders when the entire West was going through its biggest expansion phase. Building on the anti-elitism concept, these elites were now beginning to be seen as the villains in a fractured society that badly needed a person who could emerge from the "people" and lead it back to its rightful place. The biggest elites were obviously the politicians and, since the citizens have one or more ways of expressing their internal displeasure in pretty much any form of democracy, foreign policy became a very important element in the populist arsenal of rhetorics.

The multilateral security environment, with NATO at its lead, took years of painstaking work to get to the point it is today. Nations are collaborating, sharing intelligence and organizing training missions together. If one fault can be found within this process, however, is that all NATO, EU, and other such organizations have done is teach the elites that working together is good for everybody. They have never, despite EU's claims, successfully managed to convince a wide majority of their citizens that multilateralism is the way of the future and the apparent failure of trying to coin the "European citizen" term stands as proof of that. Combine that with the recent failures of some democracies and a picture is starting to form up. States are nothing without their citizens and while the elites matured into developing the framework of collective security, the people, due to a lack of understanding, began to see it as a reason for many of their problems.

2. Populism: influencing the way actors understand security

As it stands, it appears that the 2020 U.S. presidential election is attracting a very high level of scrutiny from European observers which by itself can act as proof that the 2016 lesson has been thoroughly learned this time. They now recognize that the world as a whole will have to face consequences regardless of who wins the elections and, as such, the entire world needs to be prepared for that. According to some foreign experts, Trump's first-term win did not seem as a serious security threat in the beginning because he was perceived as an unknown entity compared to his opponent. The other actors were wary of his possible behavior, but not overly worried at that moment. However, while Democratic candidate Hillary Clinton was a known and valuable asset, the personalities and policy positions of

[2] Judy Dempsey, "Populism Will Undermine the West's Security – For Putin's Benefit", in *The Washington Post*, URL: https://www.washingtonpost.com/news/global-opinions/wp/2016/11/15/populist-movments-will-undermine-the-wests-security-to-putins-benefit/, accessed on December 26, 2019.

Donald Trump and his entire team were, in large part, a mystery, and this developed the need to further understand and acquire contacts in the new White House administration[3].

Security-wise, this has also translated into an unprecedented sense of drift between the two shores of the Atlantic, especially at an ideological level. While previous administrations have most certainly had their own discrepancies with Europe, the *status quo* remained pretty much the same at all times. Since nobody can argue that the current U.S. President is not a populist leader in any way, shape, or form, his antagonistic views towards multilateralism have done nothing but increase a feeling that was already present and has been, nevertheless, given much more power due to the unencumbered support offered by arguably the most powerful man in the world. Considering that the world post-World War 2 has been heavily oriented towards multilateralism and a better communication among countries, it's fair to say that this has brought to the forefront arguments that else would have still taken a long while to unfold.

From a populist point of view, we think it's necessary to try and understand the concept in a somewhat different light rather than the theoretical, Buzan-ist standpoint that characterizes international relations where security is seen as "the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change, which they see as hostile"[4]. Rather, populism expands and shrinks this definition at the same time, lowering it to a level simple enough to be understood by the common citizen, yet complex enough to still be ideologically flexible. However, this raises a legitimate question regarding the way regular citizens understand the concept of security. A hypothesis that we have found to be adequate is laid out in the work of Valerie Sulfaro and Mark Crislip, where they argue that "absent a salient focal point, there will be no stable enemy images for most members of the mass public. Instead, perceptions of national security threats will be rooted in the politics of movement"[5]. Since politics of movement work perfectly when conflated with the flexible ideology of populism, this allows such leaders and politicians to be able to freely manipulate the concept of security, when such a concept is regarded from a citizen's point of view, at least. So if a citizen is made to believe that security is the ability of his or her state to maintain independence and functionality against actors looking to exert their influence for their own gain, it's small wonder that such augmentations coming from the leader of the White House can have such a profound impact on the whole Transatlantic relationship.

However, we can't stress enough the importance of not focusing on one single event as the determining factor that was finally able to bring populism at the forefront of international relations and allow it to have the power to change the very understanding of the concept of "security". The main element to be highlighted here is that populism does not alter what people want in their most basic state. Humans are still looking to fulfil the same needs even in terms of security and defence, now more than ever. What is changing is the foundation upon which the concept is built and it is the second time this happens in as many centuries. Following World War II, countries have worked endlessly to try and promote

[3] Erik Brattberg and David Whineray, How Europe Views Transatlantic Relations Ahead of the 2020 U.S. Election, in *Carnegie Endowment For International Peace*, 2020, URL: https://carnegieendowment.org/2020/02/20/how-europe-views-transatlantic-relations-ahead-of-2020-u.s.-election-pub-81049, accessed on August 31, 2020.

[4] Barry Buzan, "New Patterns of Global Security in the Twenty-first Century", in *International Affairs (Royal Institute of International Affairs 1944-)*, Blackwell Publishing, 1991, pp. 432-433, URL: http://www.jstor.org/stable/2621945?origin=JSTOR-pdf, accessed on December 28, 2019.

[5] Valerie A. Sulfaro, Mark N. Crislip. "How Americans Perceive Foreign Policy Threats: A Magnitude Scaling Analysis", in *Political Psychology* 18, no. 1 (1997): 103-26, URL: http://www.jstor.org/stable/3791986, accessed on August 27, 2020.

multilateralism as the means to ensure that everybody can live free and prosper. In layman's terms, democracy could only be protected by a union of actors that would join together and prevent a new war that could prove to be even more catastrophically than the last two. The recent failures of some democratic states coupled with the rise of populist values are slowly shifting the position of main referent to its original, pre-1945 owner: the state. While this is indeed the traditional way to view things, a world where the elites and the citizens do not agree in regards to the main element that acts as a shield in the face of external threats has the ability to bring about new kinds of danger. Therefore, this leads to a status quo where the state on one side and multilateralism on the other are seemingly competing against each other to claim their role as main protector. Lack of consensus here is a new and different type of danger that can lead to a worsening of the balance of what we call "*international relations".* Regardless of who is the main defender, the state or all-out multilateralism, both of them require consensus in order to work properly. If actors do not know or are unable to pool their resources and concentrate them in one spot, and they instead opt to try to promote both agendas at the same time, this could lead to a very inefficient world order going forward.

As we said, international organizations seem to have cornered themselves into a standstill due to the way they handled the meaning of security through the last half of the 20th century and almost a quarter into the next one. Since the transition from the end of the Cold War to the globalization period has been rather fast, many actors tend to remain stuck on the line of thought that sees security as a concept that is to be handled purely by the state due to its many sensitive implications. While, in itself, that is as valid a statement as it gets, it's safe to say that the world of today has given rise to a question that challenges the foundation of democracy like never before. All through the last century, countries have fought to ensure that the democratic model of governance remains the dominant form of leadership in the world and they have succeeded. However, proper leadership is hard to apply if citizens become vocally unhappy with the people chosen to govern them. Until today, political elites could certainly afford to debate and discuss the many reasons why multilateralism and international cooperation are the best ways to keep peace in the world. However, not enough attention was given to the involvement of the common citizen on the matter, at least on an informational level, and this is an issue that has serious consequences now.

Maybe it's time we use an example to get the point across. Algeria's long independence war with France and the internal conflicts that followed have led to hundreds of thousands of deaths and instilled in the Algerian people a healthy respect for law and order. As a result, the regime of former president Abdelaziz Bouteflika used this fear of war and instability in order to justify its own authoritarian measures and it worked, up to a point. As a new generation emerged, one that did not directly see and live through the horrors of conflict, the citizens became more and more dissatisfied and it all culminated in the 2019 mass riots and the ousting of the octogenarian president. This, to a certain level, is the proof of how populism is on the rise today and has become such a dominant force in international relations. Spurred by the anomalies and discrepancies that happened during World War II, international actors did not stop to transparently explain to the people what they were doing because they faced such a difficult task ahead of them: rebuilding the entire world order in a manner which ensured peace in the future. As the years went by and reality morphed into history, generations today have become more focused on the present-day achievements of their governments and their many failures as opposed to security victories from the past. Populism also contributes to this type of speech due to its ability to change sides and ideological views, vocal leaders and publications increasing the community's level of unhappiness.

Buzan talks about the three levels of security as individuals, states, and international systems while also arguing that "the security lens (…) is a broad one"[6]. Citizens will always reduce its meaning to the most basic form, the one concerning their individual needs and the ability to keep their integrity against "forces of change"[7]. As it happens, we are living in a century of deep and profound changes and the struggles of the international system, otherwise normal and understandable, are watched through the broadness of Buzan's security lens. Individuals feel the struggles of the world and need someone to be made responsible for them. States are pulled deep into the integration process yet they still have their plethora of internal issues to deal with. International systems have to try and balance all of this and somehow end up on the winning side in order to justify the nature of the world order that they have created. However, the citizens do not feel as much a part of this order as they feel that a certain governance model has been imposed on them and this is where populists start to shine. As long as the system works, there's little to be angry about. When the system goes through issues and when iconic members start pulling out of it, the people will obviously have doubts and start looking towards any justifiable explanation. The dangers of populism, to be frank, lie not in its ability to call for change but more so in the subtle influence that it exerts on the perception of the citizens and the way it paints the international security system as the cause of all problems rather than the solution. This is not to say that populist leaders completely forego any type of connections to other states but that, once they are in a dominant position, any truth that is not *their* truth becomes wrong for them. Since, once again, multilateralism relies on communication and consensus, this has the potential to bring about a long line of conflicts.

3. A threat to the transatlantic and inter-European relationship

While NATO stands to be the first that has to deal with the way populism can impact security due to its role as a provider of it, the European Union has also played a fundamental part in this process up until now. The reason why this is important is because security is not always defined with the help of military capabilities but is also, quite often, represented by how safe certain actors feel in relation to a certain event or environment. For instance, free movement is both one of EU's core values and one of the elements that is viewed today as a potential threat to the security of the continent and of the world. While international actors have strived, like we said, to emphasize the need for multilateralism and multi-state organizations that can act as guardians of a free world, the perception of the people has also continued to evolve in a slightly opposite direction. Daniel Thym argues that much of the liberties that we today associate with "intra-European" mobility" are also guaranteed by the international human rights law anyway[8].

Of course, nobody is challenging the essential role of the European Union when it comes to promoting human rights and making the continent a better place overall. However, the lack of communication and transparency that we stated before has been unable to keep up with the Western society's switch in self-perception. In other words, the considerable extension of the level of individual and collective rights is not always, at its core, directly associated with the value that international organizations bring in terms of security. Populism is innately designed to thrive in such a scenario, as its ideological flexibility allows it to point

[6] Barry Buzan, *op.cit.*, pp. 432-433.
[7] *Ibidem.*
[8] Daniel Thym, The Failure of Union Citizenship Beyond the Single Market, in: Bauböck R. (eds) *Debating European Citizenship*, IMISCOE Research Series, Springer, Cham., 2019, URL: https://doi.org/10.1007/978-3-319-89905-3_20, accessed on August 31, 2020.

fingers in every direction and always come away looking like a winner. Our belief is that at its roots, populism is named like this simply due to the already-existing trend of modern-day citizens to go back to their national roots and forego some of the more unwanted consequences of multilateralism and globalized democracy. Since security is a product of the type of relationships and bonds formed after World War II, anything that is so adaptable has to be seen as a serious threat because, at the end of the day, states cannot exist in an opposition with their own people.

Europe stands as proof of that considering how populist movements mix their Euro-scepticism with a new and fresh wave of anti-Americanism permeated in large part due to the *modus operandi* applied by the leader of the White House. This is not the only element worth considering though as populist movements and tendencies are springing out all across the continent. Regardless of the real security threats we face, their message is that the state is completely capable to take back the control it deserves and look after itself without any need of external help[9]. That was also the message that we got from the Brexit effort and Britain actually leaving the EU eventually was another blow, regardless of the consequences that will follow this event. Obviously, Donald Trump's victory was as much a message to Europe as it was to his own American continent. At a time where a reinforcement of the Transatlantic relationship was required in order to keep moving forward, "America First" acted as an all-out boost for populists around the world: those in the United States received much-needed approval that their country should always be ahead of everyone else while those around the world were once again confirmed of the perils that lie in trusting the help of others.

Another thing worth mentioning here is that populism does not only work on a citizen level but its security implications reach far wider than that. We must not forget the calls for the establishment of a European army or for the European Union as a whole to take a more hands-on approach when it comes to its security process[10]. This type of thought automatically brings internal security challenges that have to be dealt with in a yet-diplomatically fashion. Countries from the Eastern bloc do not view EU as having the ability to replace NATO when it comes to military capabilities, intelligence-sharing, or logistics and this can prove to be quite a risk going forward. The international order as a whole was created so that all the major organizations, working in conjunction, can provide security and freedom to their citizens. What populism did is make security into a sort of detachable concept that everyone can find for themselves without bothering with the needs of someone else, as if such a thing as internal and nation-only security was still possible in the 21st Century.

At this point, going at it alone is not really an option due to how connected the entire world has become and the exponential increase of elements perceived as threats. Although judging NATO or the European Union for their procedures or politics is the easy thing to do, the truth is that they are essential parts of the security architecture. When it comes to Bruxelles, a large part of the problem seems to be that it's as much a victim of populism as it is an instrument through which the ideology can spread. There's a difference that has to be made here between the beliefs of regular citizens and the actions carried out by governments. However, the entire present context coupled with the twists and turns of Brexit seem to have carried out a message that what the EU wants to do is not always aligned with national interests and objectives[11]. Among people who do not make it their every day's business to inform themselves in regards to the positions and actions of international organizations, this

[9] Judy Dempsey, *op.cit.*
[10] *Ibidem.*
[11] Mark Galeotti, *Will the populist wave wash away NATO and the European Union*, 2017, URL: https://www.nato.int/docu/review/articles/2017/01/06/will-the-populist-wave-wash-away-nato-and-the-european-union/index.html, accessed on December 28, 2019.

can raise one obvious question: Why should we be members then? While NATO undoubtedly remains the much-needed military alliance, the European Union also has certain spots that it is able to fill and it takes a collective effort to counter these emergent security threats.

Also, a lot of observers sadly still only see this issue from a political and economic perspective and that can hardly be the case anymore. As cyberspace becomes a security field regarded on level ground as the older ones, so too must the social perspective become more and more important due to the way things work today. If there is one important thing that we have learned about the nature of this new, hybrid war is that conflict today is fought much more in the fields of governance, politic, and society than it is on the actual battlefield[12]. Also, populism must not be understood as a simple and single event of bad luck that happens to fit right into the flaws of the current world order. Rather, it is as much a consequence as it is a stand-alone threat due to its very nature, as it had been evolving before the unfolding of current events but has nevertheless shifted and adapted its vision and values in order to better point out the failings of multilateralism and globalization. We are facing an enemy that is capable of changing its own vision in the eyes of the people, in the same way a broken mirror does reflect back a tad of the actual reality, yet an altered version nonetheless.

Indeed, the main threat for the future does not seem to be disintegration of international organizations as angry masses tear them to the ground but rather them fading into irrelevance as the rise of populism forces national governments to pay more and more attention to nation-only interest and objectives. A research conducted in 2016 found that many countries in Europe were clearly considering that nations would be better off if they were left to deal with their own problems at their own pace rather than trying to follow a complex and strict behavioral pattern that comes from an international entity[13]. Countries like Greece, Italy, and Poland have shown or are still showing to be extremely receptive to populist ideas and the natural spreading tendency of such concepts makes them all the more dangerous. As we said earlier, this can also impact the desire and ability of new states that want to or are thinking about joining these organizations. Since membership in the EU and NATO has become somewhat of a first step and a rite of passage for countries looking to take that decisive step towards a fruitful democracy, it's easy to see just how far the ramifications can go. Obviously, the culture and development of the prospective breeding ground will matter a great deal in terms of where populism will show its head next. However, due to the risk potential and the standalone need for European and international unity due to security purposes, a more pragmatic approach to it will surely behove us in the future.

Conclusion:
Populism blooms due to the challenges of multilateralism

We have therefore tried so far to present this complex, but understandable issue in its entirety, without leaving anything out: the state of the world today offers constant challenges to multilateralism. In order to be surpassed, these challenges require the support of the citizens. However, the people did not receive proper explanations and information when the new world order was being engineered after World War 2, so they are easily influenced now, when the entire system is struggling. Spurred by worries and the need to stabilize an environment that was left devastated by two World Wars, the international actors took painstaking efforts to convince themselves of the need for cooperation, but did not spend a

[12] *Ibidem.*
[13] Bruce Stokes, Richard Wike, Jacob Poushter, *Europeans Face the World Divided*, 2016, URL: https://www.pewresearch.org/global/2016/06/13/europeans-face-the-world-divided/, accessed on December 27, 2019.

great deal of time trying to sell this idea to their own people. This, coupled with the difficulties that the world is going through today, has led a lot of citizens to start doubting the benefits of multilateralism and of a colective system of security.

Populism is merely the materialization of this line of thought translated into its anti-elitism and anti-pluralism speech. When it comes to security implications, we can identify two main concerns that will quite possibly demand a lot of attention in the future: first, to achieve external security objectives, you need to have a stable environment at home and a continuous rise of this type of ideas may very well prove to be a threat to that. With news becoming global in a mere instant, anything that happens on one side of the globe can be read on the other side of it, and this impacts the ability of national actors to make a crisis decision due to the added amount of pressure. This conflict with its own citizens has the potential to hold down the development of a state, especially for those which do not have a strong democratic tradition. Populism can impact the understanding of security by not allowing the full use of a country's capabilities due to social strife. Since an actor that does not possess a stable base can seldom revert to exerting external influence, be it in the manner of *soft power* or *hard power*, an unaddressed populist threat has the potential to create internal contexts which will indirectly prove to be a threat in the long run.

Second, the same threat can definitely have an impact on the way that security systems are able to function at an international level. As populist champions continue to emerge and promote their speech, tensions will always be on the rise. In addition to the traditional discrepancies in the NATO-Europe relationship which are not that few to begin with, having leaders with the ability to jump from one side of the political spectrum to the other is hardly going to make for a stable environment. Security, by its very definition, needs practices and rules that can be put into place and strictly obeyed in order to be able to prepare for predictable events and answer efficiently to unpredictable ones.

As a result, we can expect *Early Warning* practices to be even more important in the future than they are today. The rise of populism seems to bring them more and more into the center of an adequate security framework for the future since the time between the emergence of a crisis and the moment when decision makers have to issue a response is significantly reduced. Trickle-down politics, simply offering bits of information to the public, is not a strategy that seems to work anymore. Anti-pluralism and anti-elitism are both volatile concepts that can be applied to both internal and external policies with just a few well-placed words. Therefore, the states will need to do an even better job when it comes to convincing their citizens about the advantages of cooperation and multilateralism, while international actors have to keep a keen eye on future prospective challenges in order to ensure they are not caught by surprise when they will undoubtedly surface.

BIBLIOGRAPHY:

1. BRATTBERG, Erik; WHINERAY, David, "How Europe Views Transatlantic Relations Ahead of the 2020 U.S. Election", *Carnegie Endowment For International Peace*, 2020, URL: https://carnegieendowment.org/2020/02/20/how-europe-views-transatlantic-relations-ahead-of-2020-u.s.-election-pub-81049
2. BUZAN, Barry, "New Patterns of Global Security in the Twenty-first Century", *International Affairs (Royal Institute of International Affairs 1944-)*, 1991, Blackwell Publishing, URL: http://www.jstor.org/stable/2621945?origin=JSTOR-pdf, 432-433
3. DEMPSEY, Judy, "Populism Will Undermine the West's Security – For Putin's Benefit", *The Washington Post*, 2016, URL: https://www.washingtonpost.com/news/global-opinions/wp/2016/11/15/populist-movments-will-undermine-the-wests-security-to-putins-benefit/

4. GALEOTTI, Mark, *Will the populist wave wash away NATO and the European Union*, 2017, URL: https://www.nato.int/docu/review/articles/2017/01/06/will-the-populist-wave-wash-away-nato-and-the-european-union/index.html
5. PLAGEMANN, Johannes; DESTRADI, Sandra, „Populism and Foreign Policy: The Case of India", *Foreign Policy Analysis*, 2019, URL: https://doi.org/10.1093/fpa/ory010
6. STOKES, Bruce; WIKE, Richard; POUSHTER, Jacob, *Europeans Face the World Divided*, 2016, URL: https://www.pewresearch.org/global/2016/06/13/europeans-face-the-world-divided/
7. SULFARO, Valerie; CRISLIP, Mark, "How Americans Perceive Foreign Policy Threats: A Magnitude Scaling Analysis", *Political Psychology*, 18/1997, no. 1, URL: http://www.jstor.org/stable/3791986, 103-26
8. THYM, Daniel, "The Failure of Union Citizenship Beyond the Single Market", 2019, Bauböck R. (eds) *Debating European Citizenship*, IMISCOE Research Series. Springer, Cham., URL: https://doi.org/10.1007/978-3-319-89905-3_20

THE POTENTIAL OF STRATEGIC COMMUNICATION IN THE PURSUIT OF NATIONAL SECURITY OBJECTIVES

Iulia COJOCARU
Ph.D. Student within "Carol I" National Defence University,
Bucharest, Romania. E-mail: iulia.cojocaru92@gmail.com

Abstract*: Under the assumption that communication is the most convenient way to know and understand the world we live in, this paper focuses on the importance of effective strategic communication, in line with the national security objectives. The potential of the communication process in achieving the desired effects has long been exploited by organizations and businesses. Nowadays, the actors in the international arena use this potential to pursue their own interests, giving rise of new threats, which in terms of security are placed under the umbrella of hybrid threats (propaganda, disinformation, fake news etc.). It is, therefore, necessary to develop new ways of combating such threats, adapted to the contemporary security environment, and to the security trends brought by current phenomena that the world is facing - such as globalization or technological advances. In this respect, international organisations such as NATO or the EU – at the regional level –, and states – at the national level –, shall endeavour to develop a framework for effective use of strategic communication. Thus, the paper aims to present solid arguments regarding the potential of strategic communication in supporting a state's instruments of power pursuing national security objectives, when it is conceived in an effective manner. The paper also emphasizes the benefits that an efficient strategic communication process can bring to a state's society, compared to the negative effects that the lack of it brings to other ones.*

Keywords*: strategic communication; vulnerabilities; countering hybrid threats; resilience.*

Introduction

In the context of globalization, supported by the evolution of high technology, the current period is characterized by dynamism, unpredictability, complexity and novelty. These phenomenon brings both advantages and disadvantages to the security environment. In the field of security studies, the aim is to provide a theoretical framework in order to minimise the adverse effects regarding how actors should understand and absorb the changes brought by globalisation and technological advances. The transition from the initial to the final state of globalization is desirable to occur smoothly, gradually and without allowing the emergence of new issues to become real security threats and risks. An example of such new issue is immigration phenomenon increased as result of frontiers openness and the need of workforce in some developed countries that, on the one hand, gives poor or endangered people the opportunity to access a better way of life, but, on the other hand, some cohesion risks rise between host communities and migrants.

The novelty in the analysis of the security environment is induced by the transition of power games from a conventional framework to a hybrid one. Thus, from a framework where rules are clear, laws are written and weapons are classic and used in plain sight, the transition is done to a framework lacking a legal basis on which the new threats can be sanctioned as well as a comprehensive theoretical foundation of how events unfold. Moreover, this

transition involves exploiting the specific vulnerabilities of peoples, targeting every citizen, not only the military trained to fight as in classical conflicts. Therefore, this paper aims to put forward arguments to support the idea that the process of strategic communication can function as a "*soft-tool*" in countering those hybrid threats addressed to people's vulnerabilities.

History to date has proven that freedom – translated in political terms into democracy – is the most conducive factor in the development of societies. Even in these circumstances, democracy still seems to have gaps in the legislative system, and in a democratic system most of the solutions to solve these problems are met with the paradox of restricting freedom. The phrase "information is power" seems to come out of the error of cliché, since assimilation, processing and interpretation of information can produce changes that may alter reality and damage public confidence in state institutions and their decisions, thus giving rise to new national vulnerabilities.

Communication is the most convenient way to know and understand the world we live in, by transferring information and subsequently by assimilating and integrating it into the thinking mechanism. Today, the channels and means of communication do not cease to multiply. In a world where imitation of successful models is a behaviour that characterizes contemporary societies, and success seems to be augmented by the constant connection with mass-media communication, which pursues recognition and exposure, we cannot neglect the potential of communication, or more precisely the way it is conceived and realized. Thus, communication becomes a two-sided coin: in a constructive sense, it can contribute to strengthening national resilience, and in a destructive sense, it can acquire the attributes of a weapon with destabilizing effects in the long term.

1. Valences of communication in the analysis of the security environment

Seen as an instrument of knowledge, communication is a way of understanding the world, by interpreting signals (whether verbal or non-verbal) and integrating them into their own system of analysis of the environment and oneself. Scientists at the Palo Alto School (California), who studied this concept around the 1950s believed that "everything is communication" and that fields such as science, art or everyday practices are sectors that communication encompasses[1]. In the paper "A logic of communication", they launch *seven axioms*, which constitute guidance for those who analyse the process. The first of these is expressed succinctly and clearly, through the phrase "communication is *inevitable*", arguing that irrespective of the will of the considered person, they participate in the permanent process of communication – taking into account that "any type of behaviour acts as a message"[2]. The second axiom briefly schematizes an important aspect of the communication process and provides a logical view of the mechanism of information interpretation, by delimiting two levels present here: the relational and the intentional levels[3]. Thus, the relationship between the transmitter and the receiver will form the basis of the interpretation of the communication intention, providing valuable clues about how the message should be processed and assimilated. The other axioms highlight the traits of communication: *continuous* – referring to the independent character of the communication in terms of cause-effect; *digital and analogue* – referring to the different form that messages have in cyberspace (digital, coded in

[1] Eugeniu Nistor, "The Axioms of Palo Alto Communication School", in *The Proceedings of the "European Integration - Between Tradition and Modernity" Congress*, pp. 956-959, "Petru Maior" University Publishing House, Tîrgu-Mureş, 2013, URL: http://www.diacronia.ro/en/indexing/details/A23451, accessed on 28.07.2020.
[2] *Ibidem.*
[3] *Ibidem.*

numbers); *symmetrical or complementary* – regarding the relationship between transmitter and receiver; *irreversible* – regarding the fact that the effect(s) produced cannot be undone, once the message has been transmitted; and *adjustable and adaptable* – regarding the way a message can be perceived.[4]

These axioms also apply in the study of communication in the analysis of the security field, where special attention is given to the interpretation of messages depending on the type of relations between participants in this process. Certainly, the interests manifested by each participant will be pursued by complex means, which will combine different strategies for achieving the proposed objectives, by adapting to contexts.

The bivalent nature of communication as regards the nature of the produced effects – constructive or destructive – stems from the extension of its basic purpose, that of pure information (where communication is thought of and expressed in an objective manner), to the management of the desired effects, in accordance with the pursued interests. If a country or, by extension, an international organisation is committed to promoting and preserving its characteristic values, then internal communication will be carried out to enhance such attitudes. On the other hand, when state or international organization interests cross own borders, the manner of conceiving the messages intended for external entities from which certain advantages are expected may acquire nuances likely to make the target vulnerable to the communicational threat. Still, the most useful way of countering these specific threats is to sustainably strengthen the education system in the sense of providing future generations with instruments as critical thinking and security culture.

2. From public communication to strategic communication

Communication, in general terms, is the process that allows the exchange of information between a transmitter and receiver(s) in order to influence the receiver and, in this sense we can anticipate its strategic character.

A first more in-depth approach to understanding the term 'strategic communication' brought some researchers to the point where they realized that although the concept had not been clearly defined by then, the need for such procedures had already been signalled in different fields of activity[5]. Furthermore, researchers have identified cases where the communication strategy, formulated in an intelligent manner, was already used by successful organisations/institutions[6]: in managerial communication to help the employees and collaborators to promote and understand the mission, vision and purpose of the company; in marketing communications in the promotion of products/services but also in attracting and retaining customers, suppliers and/or intermediaries and even in attracting outsources funds (in the case of NGOs); in public relations to support the establishment of the interrelationship framework between people, government, investors, by highlighting the role each of them has in the lives of the others; in communication technology process in order to educate employees to improve their efficiency, to reduce the number of technical errors and promote efficient use of technology; in political communication for building political consensus, or for influencing the results of the election campaigns (internationally, communication comes to the aid of public diplomacy and helps the military in the stabilisation process); in information and social marketing campaigns aimed to reduce risk-factor behaviours, or to promote actions that improve the security state of the community. To this day, companies but also state and

[4] *Ibidem.*
[5] Maria Victoria Carrillo, "Strategic Communication in the communications environment of today's organizations", in *Comunicação e Sociedade*, vol. 26, 2014, pp. 81-89.
[6] *Ibidem.*

supra-state actors have acquired strategic communication techniques into procedures and concepts that undergo continuous adaptations, according to the dynamics of the security environment.

Some specialists consider that a comparative analysis between strategic communication and traditional communication highlights at least four reasons for the strategic communication rapid occurrence[7]: the inability to obtain further benefits by using solely traditional communication, the substantial changes in the spectrum of public communication generated by the evolution of technology, the use of methods of extensive analysis of consumer behaviour by large companies and, not least, the use of strategic communication as a means of influencing to achieve interests.

Next, we will look at how strategic communication has been legislated and implemented in the security and defence spectrum by some international organisations or states.

Strategic communication in NATO and EU

After the NATO Summit in Strasbourg and Kehl in 2009, the importance of formulating a communication strategy to support the security in the area and the integrity of the Alliance is reiterated as evidenced by the statement: "It is increasingly important that the Alliance communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions. Strategic communications are an integral part of our efforts to achieve the Alliance's political and military objectives"[8]. This statement is materialized in 2014 once with the establishment of the *Centre of Excellence for Strategic Communication* in Riga, a multinational centre, which has the mission to bring a framework for strategic communication process between NATO, allied members and partners. The Centre work also aims to enhance understanding and awareness of NATO policies, missions and operations among the general public. The Centre develops on the basis of the participation of entities from different countries and sectors of activity, but also on the use of modern technology, virtual tools of analysis, research and decision-making[9].

In order to achieve the proposed objectives, this centre of excellence has developed different means of implementing and promoting the concept of strategic communication. For example, in 2015 they launched the project for the online course "Introduction to Strategic Communication"[10], aimed at the general public, which was a first step in understanding the launched concept. Moreover, it coordinates the work of a scientific journal, "Defence Strategic Communications"[11], with a free access to the online environment; a publication designed to deepen the hypostases of strategic communication, analyzing contemporary situations, events and problems. At the same time, research reports are disseminated around this topic. An example of such a report is "Disinformation as a global problem – regional perspectives", which deals with the topic of disinformation within the countries of the

[7] Kirk Hallahan, Derina Holtzhausen, Betteke van Ruler et al., "Defining Strategic Communication", in *International Journal of Strategic Communication*, No. 1, Routledge, London, 2007, pp. 9-11.

[8] ***, "About Strategic Communications", *NATO Stratcom Centre of Excellence*, URL: https://www.stratcomcoe.org/about-strategic-communications, accessed on 12.02.2020.

[9] *Ibidem.*

[10] ***, Online course "Introduction to Strategic Communications", 06.01.2015, URL: https://www.stratcomcoe.org/online-course-introduction-strategic-communications, accessed on 10.02.2020; "Introduction to the online course "Introduction to Strategic Communications"", URL: https://www.youtube.com/watch?v=fu7q-ELLP1k&feature=emb_logo, accessed on 10.02.2020.

[11] ***, Academic Journal "Defence Strategic Communications", URL: https://www.stratcomcoe.org/academic-journal-defence-strategic-communications, accessed on 10.02.2020.

European Union and those of south-east Asia, analysing the characteristics, context and anticipating trends in this phenomenon.

Another project of the centre was the development of an online educational game, "The news hero"[12], which puts the player in the position of running a publisher company, and which aims to raise awareness of the potential risks regarding the veracity of the information and the effects of its dissemination.

In the same interactive manner, a competition was launched on the theme "How to detect malicious use of video/photographic content online?"[13] in order to help understand this phenomenon and find new solutions to counter it. The stakes of the competition were a prize worth 5,000 Euros for the winning team and for the teams ranked below the first place were offered trips to Riga headquarters, making this competition even more attractive.

Moreover, to maintain a constant connection with the general public and for increased notoriety, the Centre offers the opportunity for students and young researchers to participate in internships. Also, the official website allows subscription to the newsletter of the centre, and annually there are being published summary reports – providing an analysis of the events with impact of the year.

Centre's agenda includes as well seminars, conferences, communications, which bring news and continuously deepen the concept of strategic communication.

Within the European Union, the task of coordinating the effort in public diplomacy and leading the EU's foreign and security policy lies with the European External Action Service (EEAS)[14], established in 2011, and under the control of which the *Department of Strategic Communication* was born. The European Union's Global Foreign and Security Policy Strategy[15] was developed in 2016 to provide the framework for the EU's external actions. The European Parliament drew up in the same year the document "In-depth analysis of strategic communications within the EU, with a view to countering propaganda"[16], given the preponderance of disinformation incidents pursued by Russia (in the east) and the Islamic State (in the south), which have influenced the behaviours of a target audience. In support of actions to counter Russian disinformation and propaganda, the EUvsDisinfo project[17] is developed. The projects contains reports, analyses, research results on how to identify disinformation and propaganda and how potential or actual effects on society are disseminated, following exposure to misinformation.

Moreover, a high-level conference was held in 2019 with the aim of strengthening the European Union's actions on hybrid threats, resilience and strategic communication[18]. The Conclusions presented in the final report of the conference underlined the need to continue exploiting a free common market within the European Economic Area and to further promote freedom of expression. However, the Union officials have drawn attention to the risks to

---

[12] ***, "The news hero", URL: https://www.stratcomcoe.org/news-hero, accessed on 10.02.2020.

[13] ***, "Competition: How to detect malicious use of video/photographic content online?", URL: https://www.stratcomcoe.org/virtual-competition, accessed on 10.02.2020.

[14] ***, "European External Action Service (EEAS)", URL: https://europa.eu/european-union/about-eu/institutions-bodies/eeas_ro, accessed on 13.02.2020.

[15] ***, "Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy", June 2016, URL: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, accessed on 13.02.2020.

[16] ***, "In-depth analysis – EU strategic communications with a view to counteracting propaganda", *Directorate-General For External Policies Policy Department*, 19.05.2016, URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf, accessed on 13.02.2020.

[17] ***, "EUvsDisinfo", URL: https://euvsdisinfo.eu/about/, accessed on 13.02.2020.

[18] ***, "Facing Hybrid Threats through Consolidated Resilience and Enhanced StratCom", *European Union, Institute for Security Studies*, 28.02.2019, URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Event%20Report%20-%20HRS.pdf, accessed on 16.02.2020.

which citizens of the Member States are subject, thereby affecting national resilience, critical infrastructure or zonal security. Disinformation is one of the risks identified and discussed, the phenomenon being addressed from a multitude of perspectives in this meeting. Union's ability to further promote its mission and ideological values is among the positive identified countermeasures. It must be considered, however, that there is no single approach for all Member States of the Union. Adapting the message to the strategic communication, suitable for each audience, is based on coordinates related to the identity of each nation (history, culture, linguistic nuances, religion, etc.). Media consumerism takes different forms depending on the individuals and societies to whom it is addressed. In a world where social media and related applications are gaining momentum in the consumer sphere of information, it is simpler, cheaper and easier to spread fake news and information likely to influence the behaviours of the masses.

Therefore, proactive and positive strategic communication may come as a complement to the approach of campaigns to combat and counter disinformation in the long term. In this respect, the need to strengthen *resilience in the digital spectrum* is underlined.

Strategic communication in Romanian strategic documents

Regarding Romania's alignment with the approach to the concept of strategic communication in the international environment, we can analyze the evolution of the presidential administration vision, presented in the last two versions of the National Defence Strategy of the country: for the period 2015-2019 and for the period 2020-2024.

As to the first, we refer to the *Guide of the country's national defence strategy for the period 2015-2019*[19], "a document addressed to both institutions and those familiar with the field of defence of the country and national security, especially the less informed, which invites them, in this way, to take the first step towards knowing this area"[20]. The document includes a glossary of terms designed to facilitate the understanding of the principles and concepts set out in the Strategy. Among them, for a complex approach to strategic communication, the following terms are used[21]: extended national security[22], security culture[23], security education[24] etc.

It can be seen that in Romania the need to strengthen cooperation between the citizen, community, Armed Forces and state has been officially reported since 2015. Mass education can be used in this regard, where the effect of the message transmitted to the society may be formultated in order to obtain a shared vision of the state of security.

---

[19] ***, "Ghidul Strategiei naţionale de apărare a ţării pentru perioada 2015-2019", (*Guide of the National Defence Strategy for 2015-2019*), Romanian Presidential Administration, Bucharest, 2015, URL: https://www.presidency.ro/files/userfiles/ Ghid_SNApT_2015-2019_AP.pdf, accessed on 12.02.2020, author's translation (a.t.).

[20] *Ibidem.*

[21] *Glossary of SNAp's main concepts and terms*, within the Guide of the National Defence Strategy for 2015-2019.

[22] The state of normality of the nation, ensured by protecting and promoting constitutional principles, social, economic and political stability, maintaining the rule of law, as well as by exercising the fundamental rights, freedoms and duties of citizens (a. t.) apud *SNAp Glossary*, p. 7.

[23] The totality of values, norms, attitudes or actions that determine the understanding and assimilation at the level of society of the concept of security and those derived (national security, international security, collective security, insecurity, security policy, etc) (a.t.) apud *SNAp Glossary*, p. 7.

[24] A predominantly educational dimension, through the development of a preventive attitude of the society in the personal, group and state defence and protection against risks, threats, vulnerabilities, real and potential aggressions. The way citizens regard the field of security has an essential role in managing the evolutions of the internal and international security environment (a.t.), apud *SNAp Glossary*, p. 7.

In the current version of the National Defence Strategy, strategic communication is presented as an area of the NATO-EU cooperation agenda. The Strategy includes among the directions of action within the defence dimension of Romania's efforts to achieve security objectives and national security interests. In this context, strategic communication joins the areas of cyber defence, countering hybrid and terrorist threats, resilience and military mobility[25].

The new Defence Strategy of Romania also underlines the importance of the 'state-society-citizen triad' in pursuing public interests and endeavours by placing the citizen at the heart of the action of public institutions. From here, we can anticipate *the role of public communication and, in particular, strategic communication in achieving cohesion between the three defining entities* of the national system, as the document presents hypostases that underline the need to strengthen this relationship, such as:

- "the need to develop its own rapid and effective reaction mechanisms and, inherently, a strongly dimensioned security culture - including among its citizens" (Introduction, paragraph 7) – we see here that communication is a means that can support this process, or that may even underpin it;
- "Technological developments lead to diversification and increase of complexity of security risks and threats, such as cyber attacks, information-specific activities (hostile/influence actions carried out in the public space, disinformation, the spread of fake/fabricated news etc.) and possible harmful and destabilizing effects of the import of civilian technologies in asymmetric and hybrid actions, generating new security challenges" (Introduction, paragraph 8). This sentence supporting the previous paragraph, as a concrete argument for real threats to the civilian population and fighting against them requires strengthening the mentioned relationship, where communication is an important tool that can be used in this regard;
- "In the social field, the security environment is influenced by increasing individualism and isolation in cyberspace, the vulnerability of online social media to information warfare and migration" (Introduction, paragraph 9). The phrase highlights vulnerabilities already reported at present, with the possibility of propagation in the future, related to methods of communication that are effective for users of social media, which may fall into the trap of assimilating malicious information and may end up isolating themselves in the online environment that they consider safer, but which is actually more unpredictable and prone to vulnerability;
- "The attachment of Romanian citizens to the values of our community of belonging is a favourable factor for ensuring extensive national security, but it must be correlated with measures and actions aimed at increasing citizens' confidence in national institutions and values, in the rationality and efficiency of the act of governance, in the values and capacity of the Romanian society to endure and progress in the political, economic, social, cultural, democratic fields according to the rule of law, a free society, performant from the economic, social and cultural point of view, environmentally sustainable, inclusive in relation to all its citizens" (Chapter 1, 1.1., paragraph 40). This sequence considers the opinion polls[26] which show that the Romanian people do not trust the institutions and decisions of the state, *the emergence of many groups, pages and posts* in online media of anti-nationalist ideas, which emphasize the problem of corruption in Romania. The importance of strengthening the confidence of the population *is reiterated.* Here we see communication as a way to support

[25] ***, *National Strategy for the Defence of the Country for 2020-2024*, Presidential Administration, July 1, 2020, p. 32.
[26] ***, "Public Opinion in Romania", *Center for Insights in Survey Research*, 7th May – 2nd June, 2018, URL: https://www.iri.org/sites/default/files/final_romania_poll_presentation.pdf, accessed on 13.02.2020.

the rehabilitation of this image, to disseminate information on the actions of the State so as to remedy the mentioned problem in a transparent manner;

Later on, the Strategy presents concrete means and methods planned for the period 2020-2024 from the main directives set out above. Thus, in order to develop "effective tools for strengthening *societal resilience*"[27], objectives are presented to be pursued through a method of communication designed in an intelligent, efficient way, with messages adapted to the effect it aims to achieve. Some of these objectives are[28]:

- improving awareness of hostile/influenced actions in the public space through classical or online media or think-tanks, difficult to manage when new security-impact factors such as fake news, for which the source is often difficult to identify and attribute;
- facilitating the sizing of accessible and transparent public tools to expose sources of misinformation, their products and narratives;
- increasing the capacity of educational, research, think-tanks and media institutions to identify and combat disinformation movements supported by hostile state or non-state actors;
- increasing the level of functional literacy for the development of critical thinking and for reducing the vulnerability of the population to the phenomenon of spreading false information, which can have negative consequences for national security;
- starting extensive education programmes in elementary and secondary schools, in the sphere of digital skills and online security, and for the development of the necessary abilities to combat false information, so as to diminish the vulnerability of the young generation to such hybrid challenges, with the effect of increasing societal resilience.

These objectives are based on security education. Education is the result of communication, and in the contemporary environment, characterised by innovation, we anticipate that the feedback received (in this case) from the population can be equally fruitful, avoiding the error of a single direction of the communication process and supporting in this respect the development of a mechanism with the ability for self-regulation and adaptation in the state-society-citizen triad.

3. Strategic communication and national vulnerabilities

Public intelligence is the ability of the masses to adapt to new trends and challenges (as a quick response to changes in the security environment), to balance and self-regulate with current collective requirements and needs, to be able to solve problems as efficiently as possible, using the minimum of effort and resources, without generating new problems[29].

In this respect, we can analyse the phenomenon of the refugee crisis. As a result of threats to personal integrity to the civilian population in conflict zones and according to human rights[30], resettlement measures have been adopted for citizens at risk. The social benefit in this case was to minimise the loss of civilian lives, mobilising existing resources, with a view to building and strengthening infrastructure for this purpose. Solving this problem, however, in many cases has generated new ones, this time the risks, threats and negative effects targeting the host population. On the other hand, some states have been able to predict the potential risks of accepting the role of host people, thus refusing the

[27] ***, *National Strategy for the Defense of the Country for 2020-2024*, Presidential Administration, 1 July 2020, point 49, p. 11.
[28] *Ibidem.*
[29] Dumitru Iacob, *Transformation of peace and war: National defence - new risks and vulnerabilities*, Tritonic Publishing House, Bucharest, 2017, p. 126.
[30] ***, *Universal Declaration of Human Rights*, United Nations, URL: https://www.un.org/en/universal-declaration-human-rights/index.html, accessed on 02.01.2020.

humanitarian appeal of the United Nations to participate in this mobilization[31], but which, nevertheless, has left behind numerous unresolved resettlement requests, maintaining the threat towards the integrity of civilian citizens in conflict zones. This could be one of the situations in which the need to develop a public communication strategy in an intelligent manner that contributes to strengthening feeling and security is highlighted for both sides interacting with the stated problem. The attitude can be, and in this case must be *educated*, according to the individual, collective and natural purpose of living safely. Here we consider *strategic intercultural communication* to be an instrument that could facilitate cohesion and cooperation between the two societal elements of the stated process (refugees and the society of the host nation).

In order to identify ways of evolution for the societies, it is necessary to understand that a smart society promotes and encourages critical thinking and is supported by intelligent people, open to new solutions and complex ways of dealing with situations[32]. Moreover, a smart society must identify those successful procedural and strategic models, also using the lessons learned throughout history, the theories demonstrated by extensive research, the experiences of other counterparts, exploiting all information and adapting it to the current status and contexts in which it takes place.

It should not surprise us that a good example of this is the Americans. As a newer civilization compared to European or Asian, for example, they practiced taking over foreign models and teachings and adapted them to the needs of the people and the American context, and this has perhaps brought them to the position of great power they have today. So if we consider that defence strategies throughout their evolution, it is clearly seen that the potential of a seemingly less trained and outnumbered enemy (terrorist groups) has not been underestimated but, on the contrary, they have analysed the radicalization strategies used by extremists thus to be able to develop not only a method of defence against hybrid threats of this kind, but also to develop and appropriate (by adaptation) their own strategy.Therefore, their strategy is better outlined and documented and based on the enemy's tactics, but also strengthens the nation's desire for a safer country.

4. Impact of uneffective strategic communication in Romania

The ideal society is when any citizen can draw the correct conclusions about the course of events happening within the community, thus in a functional level there can be developed individual and collective strategies of preservation and of living in peace and harmony. Consequently, the society can work as a resilient holistic system with the capacity for self-adaptation and self-regulation according to past experience and obtained results.

In Romania, this ideal society seems to be far from reality. The experience of the last generations has led the Romanian people to use their collective intelligence to develop more of a self-defence strategy towards the state than a collective development strategy with and within this state.

The society's *confidence* in high-level decisions is deeply affected by the contradictory directions promoted simultaneously by the different political parties. For example, the current conception is that the Romanian state is separated from its people, their interests not only differ but are quite contradictory and these are expreseed in poor communication, lack of dialogues and transparency in political speeches between

[31] ***, "Statistics – Hungary", Hungarian Helsinki Committee, URL: https://www.asylumineurope.org/ reports/country/ hungary/statistics, accessed on 10.01.2020.
[32] Dumitru Iacob, *op. cit.*

representatives of the state and society, delivering content without expecting feedback from the audience, or public lie promoted as a technique of political act.

Also, the lack of confidence in the directions promoted by the state and the attitude of the state (sometimes careless, perhaps even abusive) to the needs of society is reflected here in *collective frustration*. It can be demonstrated once again that the theory that "individual security is affected both positively and negatively by the state, and the grounds of this disharmony between individual and national security are a permanent contradiction"[33].

As a result, in Romania, the lack of effective public communication or strategic communication has generated the lack of civil population confidence in the Romanian state34, collective frustration, social imbalance, we can even say vulnerabilities regarding the national security. Romania's entry into the European Union was a good opportunity to raise awareness of this situation. The year of Romania's accession, 2007, coincides with the year in which the highest number of emigrants from Romania were recorded[35]. About half a million Romanians[36] in their pursuit to have a better life have left in more developed countries of the Union, as confirmed by official data provided by the National Statistical Institute.

Romania continues to be a country of emigration, this phenomenon being the second main cause of the country's population reduction. Its balance of international migration in 2018 was negative, with the number of emigrants exceeding the number of imigrants by more than 57,000 people[37]. Also, about half of young people population under the age of 30 consider leaving Romania [38].This trend poses a risk to the stability and security of our country. Moreover, at the "Romanian Business Leaders" Summit in 2018, Iulian Stănescu, Doctor of Sociology, launched the following statement: "In peacetime, Romania, in the last 30 years, has lost more people than in each of the two world wars ... People leave Romania and leave for good in search of a better life, which they cannot achieve here"[39]. It is estimated that if these mass movements persist, Romania's population will shrink from 19.2 (currently[40]) to 13.8 million in 2060[41] (about 30% less). The effect of mass migration can have devastating effects not only on the economy, but also on the country's culture, national identity, integrity and security, ultimately.

Searching for the reason behind this situation, we can say that the roots of the problem lie in *education*. During communism, patriotism was illustrated in schools in an idyllic form,

---

[33] Barry Buzan, "Peoples, states and fear", Cartier Publishing House, 2000, p. 65.

[34] ***, "Public Opinion in Romania", *Center for Insights in Survey Research*, 7 May – 2 June 2018, URL: https://www.iri.org/sites/default/files/final_romania_poll_presentation.pdf, accessed on 27.07.2020.

[35] A.N.: "The stock of emigrants consists of all persons with Romanian citizenship who had their habitual residence on the territory of another state for a period of at least 12 months at a given time", National Institute of Statistics, in "Exploratory study on migration stocks", URL: http://www.insse.ro/cms/sites/default/files/Statistici-Experimentale/studiu_exploratoriu _metode_estimare_stoc_migratie.pdf, accessed on 14.02.2020.

[36] Raluca Toma (Median Research Centre), "The real dimension of emigration from Romania. What we know and what we don't know about how big the "diaspora" is", in *Libertatea*, 16.02.2020, URL: https://www.libertatea.ro/stiri/dimensiunea-emigratiei-din-romania-ce-stim-si-ce-nu-despre-cat-de-mare-e-diaspora-2885018, accessed on 18.02.2020.

[37] *Ibidem.*

[38] Raluca Ion, "The real drama of this country: 50% of young people under 30 want to leave Romania", in *Republica*, 16.03.2018, URL: https://republica.ro/adevarata-drama-a-acestei-tari-50-dintre-tinerii-sub-30-de-ani-vor-sa-paraseasca-romania, accessed on 18.02.2020.

[39] *Ibidem.*

[40] ***, "Romania Population", in *Worldometers*, URL: https://www.worldometers.info/world-population/romania-population/, accessed on 29.07.2020.

[41] ***, "*Demographic Scenarios for The EU Migration, Population and Education*", Joint Research Centre (JRC), the European Commission's science and knowledge service in partnership with the International Institute for Applied Systems Analysis (IIASA), aprilie 2019, URL: file:///C:/Users/cojocaru.iulia/Downloads/demographic_online_20190527.pdf, accessed on 18.02.2020.

far from the true feeling that the regime instilled in the nation in which students were obliged to display a positive attitude towards any direction drawn by the system, without having the right of opinion, and any intention of ideology disapproval was severely sanctioned. It is understandable why after the 1989 revolution, the attitude of students, thinkers, artists – towards the patriotic sense – was completely diverted.

Democracy in Romania meant for many an opportunity to freely express frustrations accumulated during the years when public opinion was forbidden. The sudden liberty to be able to write and publish freely and to openly express their political options erupted in a new form of exaggeration, this time in reverse, in which patriotic movements are more hastily avoided, in an attempt to bypass a cliché used before the '90. Also, owed to the lack of democratic maturity hostile attitude towards the regime was wrongly propagated towards the sentiment of nationalism. In comparision, we can see how patriotic sentiment deeply rooted in the consciousness of a democratic nation (USA) can cause a people to strengthen their relationship with the institution of the state. The reason for this difference in situations is precisely intelligent communication, thus the purpose of civic education is accomplished when the information transmitted is assimilated according to the existent society ideology when its meaning is consistent with the direction in which each citizen sets personal goals.

Conclusions

In order to find a way to ground a security culture in people's conscience, we must first find and be able to express a common ideology, a unitary purpose. Who are we? What do we want? What are the values in which we believe, that define us, that identify us, and for which, throughout history, generations have fought to be preserved? If we can find the answers to these questions both in the family, in the education of the first "at home" years, then in the education of the institutionalized environment, but also in the attitude of the state towards the state of the nation, of society and of the individuals who compose it, then we can say that there is a common sense, a single direction, with the same purpose for both the state and the individual.

We see *communication* as the most used way in which humans act and react so as to understand the environment and events with major impact in the world. Thus, in line with the objectives proposed in the strategic documents both at the level of the international organisations of which Romania is part of (NATO, EU), but also under its National Defence Strategy, we believe that it is necessary to develop an effective strategic communication process. This is aimed at improving confidence in the state's actions by providing transparency and a responsive framework of state-citizen relation and therefore eliminating collective frustration of people perpetuated by perceived careless or abusive behaviour of state. In order to minimise such vulnerabilities are used instruments to strengthen the security culture, to develop critical thinking, and to combat hybrid threats - such as disinformation or propanganda.

BIBLIOGRAPHY:

1. ***, "About Strategic Communications", *NATO Stratcom Centre of Excellence*, URL: https://www.stratcomcoe.org/about-strategic-communications
2. ***, "*Demographic Scenarios for The EU Migration, Population and Education*", Joint Research Centre (JRC), the European Commission's science and knowledge service in partnership with the International Institute for Applied Systems Analysis (IIASA), aprilie 2019, URL: file:///C:/Users/cojocaru.iulia/Downloads/demographic_online_20190527.pdf
3. ***, "EUvsDisinfo", URL: https://euvsdisinfo.eu/about/

4. ***, "Facing Hybrid Threats through Consolidated Resilience and Enhanced StratCom", *European Union, Institute for Security Studies*, 28.02.2019, URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Event%20Report%20-%20HRS.pdf
5. ***, "In-depth analysis – EU strategic communications with a view to counteracting propaganda", *Directorate-General For External Policies Policy Department*, 19.05.2016, URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)57808_EN.pdf
6. ***, "Romania Population", în *Worldometers*, URL: https://www.worldometers.info/world-population/romania-population/
7. ***, "European External Action Service (EEAS)", URL: https://europa.eu/european-union/about-eu/institutions-bodies/eeas_ro
8. ***, "Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy", June 2016, URL: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
9. ***, "Statistics–Hungary", Hungarian Helsinki Committee, URL: https://www.asylumineurope.org/reports/country/hungary/statistics
10. ***, *Guide of National Defence Strategy for 2015-2019*, Romanian Presidential Administration, Bucharest, 2015, URL: https://www.presidency.ro/files/userfiles/Ghid_SNApT_2015-2019_AP.pdf, accessed on 12.02.2020.
11. ***, *Radicalisation Awareness Network – Issue Paper Counter Narratives and Alternative Narratives*, Institute for Strategic Dialogue in cooperation with RAN Centre, 01.10.2015, URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_cn_oct2015_en.pdf
12. ***, *U.S. National Strategy for Public Diplomacy and Strategic Communication*, 2007, URL: https://2001-2009.state.gov/documents/organization/87427.pdf
13. ***, *Universal Declaration of Human Rights*, United Nations, URL: https://www.un.org/en/universal-declaration-human-rights/index.html
14. BUZAN, Barry, „Oamenii, statele și frica", Cartier Publishing House, 2000.
15. CHELCEA, Septimiu, "Introducere în viața socială", Publishing House of the National Institute of Information, Bucharest, 1995.
16. HALLAHAN, Kirk et al., "Defining Strategic Communication", in *International Journal of Strategic Communication*, Routledge, 08.09.2010, URL: https://www.researchgate.net/publication/241730557_Defining_Strategic_Communication/link/0a85e53a585bc6cee8000000/download
17. IACOB, Dumitru, *Transformation of peace and war: National defense - new risks and vulnerabilities*, Tritonic Publishing House, Bucharest, 2017.
18. ION, Raluca, "The real drama of this country: 50% of young people under 30 want to leave Romania", in *Republica*, 16.03.2018, URL: https://republica.ro/adevarata-drama-a-acestei-tari-50-dintre-tinerii-sub-30-de-ani-vor-sa-paraseasca-romania
19. LIM, Rachel, "Disinformation as a Global Problem – Regional Perspectives", January 2020, URL: https://www.stratcomcoe.org/disinformation-global-problem-regional-perspectives
20. TOMA, Raluca, "The real dimension of emigration from Romania. What we know and what we don't know about how big the "diaspora" is", in *Libertatea*, 16.02.2020, URL: https://www.libertatea.ro/stiri/dimensiunea-emigratiei-din-romania-ce-stim-si-ce-nu-despre-cat-de-mare-e-diaspora-2885018

CURRENTS OF THOUGHT REGARDING THE STUDY OF SECURITY

Andrada ILIE
Ph.D. Student within "Alexandru Ioan Cuza" Police Academy,
Bucharest, Romania. E-mail: roandrablue@yahoo.com

Abstract**:** *Over time, there have been several theories of knowledge that have generated individual definitions of security. This paper presents a brief overview of the main such views on security. The first theory mentioned is positivism which implies an objective approach, based on natural scientific methods in which concepts such as: balance of power, number of military forces and interaction between states are used. Beginning with constructivism, the paper focuses on postmodernism, as it is a concept built around the idea that the world is a product of social interactions. This theory has led to the idea of building security in the contemporary international political process, starting from "security" and "security threats". The paper recalls the Copenhagen School highlighted through the number and scope found for the term "security".*

Keywords*: security; security construction; positivism; Copenhagen School; postmodernism.*

Introduction

In the traditional approach to the study of security in the nineteenth and twentieth centuries, security was understood as military art because war was understood as a primary and permanent function. Through this concept, the "natural" state was one of war and the intermediate one was peace.

The definition of security from this perspective is given by Stephen Walt[1] (1991), one of the realist theorists, a current of thought to be explained in a separate subchapter. The author believes that security enhances military capabilities, security and control of the armed forces of the state. So, security equals peace and conflict prevention by military means (means of deterrence, non-offensive defend etc.) establishing a middle-state position, which is being restricted by the security application to the military domain.

The sphere of national security is simply huge and faces five distinct sectors: economic, environmental, political, military and societal. Economic security refers to the state's ability to access the strategic resources and markets needed to maintain its power and well-being. Environmental protection refers to the quality of the biosphere as a precondition for the continuity of a "human life on earth". Political security refers to the ideological, institutional and physical stability of the state. It also manages the military instrument and uses it whenever necessary. Social security covers "the preservation, inacceptable conditions of progress, of traditional linguistic modes, culture and religion, national identity and customs".[2]

Definitions of security have been developed on the basis of several currents of thought, the most important of which are: constructivism, positivism and postmodernism. The

[1] Walt S. M., *Renaissance of Security Studies* in *International Studies Quarterly*, Vol. 35, 1991, pp. 211-239.
[2] David C. P., *Security. Rethinking. No threats, no politics*, Montreal, Publishing house: Fides, 2002, p. 37.

paper addresses mainly constructivism and postmodernism, because based on them, the very concept of security knows new dimensions. Constructivism comes with the novelty that security refers to non-military issues, starting from the idea that social facts are human creations, and that the social structure manifests itself not only through the material structure, but also through the international community. In their definitions, constructivists start from the premise that norms, customs, culture and learning can change the behaviors and interests of a country's citizens.

The modern construction of security comes from postmodernist thinking that revolves around the idea that the world is a product of social interactions. The paper addresses this issue through the Copenhagen School which has been highlighted by the number and scope of the term "security".

1. Positivism and constructivism

In positivism, the study of security has an objective approach, based on natural scientific methods in which concepts such as: balance of power, number of military forces and interaction between states are used. The difference between the traditionalist and the positivist approach is that, in addition to the emphasis on military issues, it also refers to non-military ones. Constructivism is based on the idea that the world is the product of social interaction, and this interaction can neither be measured nor analyzed by any scientific means that have been used by positivists. The working tool of the constructivists is constituted by the subjective ontology and the objective epistemology. Constructivism emphasizes that social facts are human creations, and that the social structure manifests itself not only through the material structure, but also through the international community. The social structure has three components: common knowledge, material resources and practices.[3] Without denying the material basis of society, constructivism emphasizes the function of ideas, because ideas are the cornerstones of the material world and can change human behavior. Human activities are carried out through the exchange of knowledge, material culture being a manifestation of this activity.[4] Constructivism believes that norms, customs, culture and learning can change the behaviors and interests of a country's citizens. Unlike rationalism, which sees anarchy as an inevitable result of self-help, constructivism sees anarchy created by the state, and just as susceptible to change through state intervention.[5]

The collapse of the bipolar world during the Cold War unleashed a variety of challenges to national security, including forces derived from phenomenon or events such as globalization and ethnic struggle. These new challenges are deeply affected by the issues that deal with the rules in which they relate to identity and social culture. The impact of these norms and identities has been ignored or accepted at face value by traditional theories. In conclusion, Christian Reus-Smit writes that “not only did the end of the Cold War raise new and interesting questions about world politics ..., the failure of rationalism to explain recent systemic transformations encouraged this new generation of scientists to review old questions and problems so long viewed through neorealism and neoliberalism”.[6]

[3] Wendt A., *Constructing International Politics. International Security*, Vol.20, 1995, p. 73.
[4] Adler E., Barnett, M.N. , *Security Community.* Cambridge: Cambridge University Press, 1998, p. 8.
[5] Wendt A., *op.cit*, p. 76.
[6] Reus-Smit, C. *Constructivism in Theories of International Relations, 2nd ed.*, New York, Publishing house Palgrave: Scott Burchill, 2001, p. 216.

Katzenstein[7] made an attempt to merge constructivist theory with practice earlier. This attempt was presented in the book "Culture of National Security - norms and identity in world politics".

By using the concept of constructivism, the notions of security were reinterpreted. All knowledge is composed of social structures that guide the nature of knowledge and social significance. Both are based on human perception, which plays a decisive role in all human actions. The concept of human security has gradually developed, through a series of academic initiatives and reports, by independent multinational commissions of experts, academics and intellectuals. For example, non-governmental organizations (NGOs) and civil society in general play a major role in the study of advocacy in human security issues and are involved in virtually all human security issues.[8] Over the years, the collective efforts of various ad hoc campaigns have led to the signing of the 1997 Ottawa Convention banning anti-personnel landmines, as well as the creation of the International Criminal Court in 1998.[9] The emergence of the concept of human security reflects, unlike the influence of national security, the influence of values and norms on security studies. This also demonstrates a change in international relations, identities and interests of states.

Table no. 1: Applying constructivist visualizations of human security[10]

Researcher	Vision	Presumtion	Use for security
Alexander Wendt	Collectiveidentity	interdependence between forms of collective identitypromotes cooperation	Human security is derived from the values of collective identity
Nicholas Onuf	language and rules	The power of knowing and shaping norms through the process of interaction	Security comes from knowledge transformed from language
GeertHofstede	Culture	Rules, institutions and values change a country's preferences	The practice of human security is derived from changing a country's preferences
Peter Katzenstein	Cultural identity	National identity changes the interests and actions of a country	Security is derived from shaping culture and identity

2. Postmodernism

Postmodernism is a concept built around the idea that the world is a product of social interactions. It cannot be known due to subjective ontology and epistemology. Researchers of this current have raised several issues regarding the role of the positivist current in the field of

[7] Katzenstein, P. J., *The Culture of National Security: Norms and Identity in World Politics*, New York, Columbia University Press Publishing house, 1996.
[8] Sané P., *Rethinking Human Security*, apud M. C. Goucha, *Rethinking Human Security*, pp. 5-6, Chichester, UK, Wiley-Blackwell Publishing house, 2008.
[9] Tadjbakhsh S., *Human Security: Concepts and Implications*, London, Routledge Publishing house, 2007, p. 23.
[10] Yu-tai Tsai, "The emergence of human security: A constructivist view", *International Journal of Peace Studies*, Volume 14, No. 2, Autumn/Winter 2009, URL: https://www.gmu.edu/programs/icar/ijps/vol14_2/TSAI%20-%2014n2%20IJPS.pdfp.25, accessed on May 12, 2020.

security in several ways of study: historiographical, methodological, ontological, epistemological and normative. Instead, they took over some constructivist ideas, especially those referring to the ambiguity of positivism in security studies.

The construction of security in the contemporary international political process leads to the fact that "security" and "security threats" are highlighted especially in political contexts increasingly transformed by the Copenhagen School approach which provides an analytical framework for the analysis of its research.

The Copenhagen school has been particularly successful in developing a concept in international relations thinking, highlighted by the number and scope of the term "security" or its variants. Security was applied to analyzes of the behavior of the state's foreign policy, to the construction of transnational crime, security threats.[11] Recent trends in post-structural security analysis have been associated with the notion of "exception" and draw strong parallels with the Copenhagen view of security as a process that has a problem beyond or outside "normal" policy.

The concept of security first entered the field of international relations and was developed by Ole Wæver in the mid-1990s. In its definition, security is one of the three central concepts for sectors called "regional security complexes". He took over the concept and elaborated it extensively in his 1998[12] book where he offered a new framework of analysis. Wæver originally defined security as an "act of speaking," as a form of linguistic representation. Later, Wæver viewed security as a normative imperative of insecurity (removing issues from the security agenda). For Wæver, "security" was the opposite of "politics", the latter implying the possibility of more open engagement and dialogue.[13]

Over time, there have been, of course, a number of other attempts to develop the concept of security, especially in locating the different dynamics of securitization in different contexts or 'sectors'.[14]

Opponents, such as Didier Bigo, formed the so-called "Paris School"[15]. For these theorists, security is built and applied to various aspects and fields. They stated that "in order to participate in the security study it is necessary to focus on the creation of networks of (in) security professionals, of systems that generate and produce productive power in their practice."[16] This is in opposition to the original concept of security, in which security practices follow speech acts.

"Sectoralization" or sectoral analysis is a method whose first serious development dates back to the publication of "The Logic of Anarchy" by Buzan, Jones and Little in 1993. It is a way to analyze the international system by activity. Each sector focuses on national security, and the nature of the threat varies within each sector and affects the security of the state actor in a specific way. Sectors are not subsystems, but analytical lenses through which the researcher investigates the state of the whole system with respect to a certain referent. Moreover, sectoralization allows a complete image of the entire system through a selected lens. The lens metaphor is very useful. Indeed, "the function of the sectors is identical to that of the lenses: each offers a vision of the whole that insists on certain characteristics, neglects

[11] Tadjbakhsh, *Idem*, p. 25.
[12] *Ibidem*, pp.7-56.
[13] *Ibidem*, pp.65-76.
[14] B. Buzan, *Peoples, states and fear*, Republic of Moldova, Cartier Publishing house, 2000.
[15] Representative: Didier Bigo, Jef Huysmans, Anastasia Tsoukalași Thierry Balzacq.
[16] Bigo, D., *Security and Immigration: Towards a Critique of the Governmentality of Unease* in *Alternatives 27*, 2002, pp 63-92.

others and sometimes even hides them."[17] Finally, sectoralization makes it possible, to a large extent, to control the abundance of variables.

In the context of globalization and the transformations brought about by the end of the Cold War (the collapse of communism, the reunification of Germany, the dismemberment of the Soviet Union and the onset of regional conflicts in Europe) we are now witnessing a shift of security analysis in the traditional modern, non-military, individual-oriented meaning. The European Union is a particular case of the relocation of the security analysis center between international organizations as a result of the centripetal evolution process.

During the Cold War years, the main security threats came from political and military areas. Thus, security was defined in military terms, reflecting the main concerns of the two opposing blocs (east-west). From this perspective, the reference object of security was the state, which should have ensured the existence of security. The dominant theoretical perspectives were realism and liberalism.[18] Realism describes the world order "as a system in which the self-interested actors of a state under anarchy compete."[19] This understanding of the world order has a direct effect on the definition of security as a feature of this anarchy. Realism has limited security studies in examining geo-strategic arrangements as a source of global systemic change.[20] This ignores the role of collective identities that have influenced the security strategy. While realism addressed security and war issues, liberalism focused on economic issues between states and international politics. Security is ensured through formal and *ad hoc* arrangements. With the development of institutional liberalism, a current close to realism, a broader approach to security began to be encouraged, starting with the type of actors involved, as well as the types of threats they might face. Interstate relations are determined by military power and leaders, as decision makers act rationally, based on the decision considered optimal, are marked by uncertainty, because decisions are made under anarchy.[21] During the 1980s, the first trends in the re-significance of security studies emerged, starting with, on the one hand, international political economy, which had to provide explanations for the turmoil generated by the globalization process, and, on the other, the social sciences, which were to provide plausible explanations for the new dimensions on the security agenda, such as identity, ethnicity, religion, poverty, terrorism, organized crime, environmental degradation, and so on.[22]

Globalization generates political fragmentation, which is a source of instability and insecurity. The process that mitigates the impact of globalization is called regionalization. Regionalization can be defined through the borders of states.[23] Through globalization, states are beginning to have additional external responsibilities as some of their internal attributes are diminished. On the one hand, political fragmentation increases the number of states and entities to be states; on the other hand, globalization increases the interdependence between states, that is, the number and intensity of relations between them. The response of the international system to these changes is visible through the increase in the number of

[17] Buzan B., Wilde J., Wæver O., *Security: A New Framework for Analysis*, Boulder, Rienner Publishing house, 1998, p. 65.
[18] Griffiths, S. M., International relations, Schools, currents, thinkers, Bucharest, Publishing house: Ziua, 2003, pp. 17-183.
[19] Baldwin, D. A., *Neorealism and Neoliberalism*, New York, Publishing house Columbia University Press, 1993, pp.1-25.
[20] Gheciu, A. *Security Institutions as Agents of Socialization? NATO*, în "*New Europe. International Organization*", nr. 59, 2005, pp. 973-1012.
[21] Keohane, R.O., Nye, J.S., *Power and Interdependence* în *International Organization, Vol. 41*, 2001, p. 151.
[22] Savu, I. N., *Security studies*, Bucharest, Regional Centre of Studies, 2005, p. 29.
[23] Bădescu I., Dungaciu, D., *Sociology and geopolitics of the border*, Bucharest, Publishing house: Blue Flower, 1995, pp. 303-337.

international regimes and through the crystallization at the regional level of security complexes. For the new challenges, the international system reacts by strengthening security regimes and regionalizing security. Along with decolonization, the level of regional security has begun to become autonomous and to impose itself in international relations.

The theory of the regional security complex offers a new interpretation of the security structure and distinguishes between the level of interaction of global powers (which can transcend distance) and the interaction at the level of the subsystem of small powers whose environment is the local region. The main idea of the regional security complex is that the most dangerous threats and interdependent security are shaped by a group of states that form a security complex.

Subsequently, the issue of regional security was supplemented by the same author and appropriated by the Copenhagen School. The most widely used definition of a regional security complex is that of 2003, given by B. Buzan and O. Weaver, who finalized a first definition: "a set of units whose major security and security processes are interdependent in a such interdependence that the security issues of the component units cannot be reasonably analyzed or decided separately from each other".[24] This approach manages, despite the criticisms, to be an important step forward and an argument for security analysis as a concept of social sciences. Although in the analysis of security complexes the researchers start from the premise that the state is the reference object of security, by emphasizing the threats of a type of society it can be considered that these categories of problems allow other reference objects to be analyzed besides the state security companies. The model proposed by the representatives of the Copenhagen School starts from the finding of the interdependence of security and the perception of insecurity, which is accentuated in correlation with geographical proximity. In order to be able to identify security complexes, it should also examine how a particular region is delimited. This was defined as "a coherent territory in terms of space, composed of two or more states". Also, "sub-region is a part of such a region and may include several states (but less than the total number of states in the region) or may have a transnational composition (a set of states, parts of certain states or both). Micro-districts refer to the unitary level below/or within the borders of a state".[25] According to B. Buzan, in terms of security, a region means that a distinct and significant security subsystem that consists of a group of states that were meant to be in those of geographical proximity against each other.[26]

Conclusions

The renewal of the security studies initiated by Barry Buzan takes as a starting point the dissatisfaction and the need to adapt the theories to the contemporary global reality. The broader security ontology he conceptualized is now inevitable. It is based on the idea that the survival of states is no longer threatened only by military factors, but that it is now necessary to integrate political, economic, environmental and societal considerations. This last aspect of the security theory of the Copenhagen School interests us. It connects national security and national identity, making it an integral part of the former. Traditionally limited to the military sector, the idea of national security is today partly conditioned by the security of the nation, the main provider of identity content.

Through the theoretical subversions it has imposed, the Copenhagen School has placed itself in opposition to the dominant security studies: a critique of the dominant theories

[24] Buzan B., Wilde J., Wæver O., *op.cit*., p. 44.
[25] *Idem*, p. 36.
[26] Buzan, B. *Popoarele, statele şi teama.* Republica Moldova, Editura Cartier, 2000, p. 194.

of security, however, remains dominant if we relate it to security studies criticism or critical constructivism. The absence of a critical epistemology about the representation of the role and place of science in societies prevents Buzan from identifying the full implications of his theoretical conclusions. The lack of reflexivity in scientific practice limits the scope of his critique of security discourses that end up being reproduced without analyzing the causes of their social forces. The errors in definition of the premises for the notion of social security make even more vague a theory whose force lies not in its explanatory power, but in its prospective and prescriptive character. As such, far from being an open concept, the concept of social security carries with it the common political presuppositions found in the discourse on identity. The security perspective applied, for instance, to international migration makes it impossible to adequately theorize these phenomena and their consequences: the field of security does not seek means of making peace, but rather methods of managing a state of war.

BIBLIOGRAPHY:

1. ADLER, E., BARNETT, M.N., *Security Community*, Cambridge University Press, 1998.
2. BALDWIN, D. A., *Neorealism and Neoliberalism*, New York, Columbia University Press, 1993.
3. BĂDESCU I., DUNGACIU, D., *Sociology and geopolitics of the border*, Bucharest, Floare Albastră Publishing house, 1995.
4. BIGO, D., "Security and Immigration: Towards a Critique of the Governmentality of Unease", in *Alternatives*, no. 27, 2002.
5. BUZAN, B., *Peoples, states and fear*, Republic of Moldova, Cartier Publishing house, 2000.
6. BUZAN, B., Wilde, J., Wæver, O., Security: A New Framework for Analysis, Boulder, Publishing house L. Rienner, 1998.
7. DAVID, C. P., *Security. Rethinking. No threats, no politics*, Montreal, Publishing house: Fides, 2002.
8. GHECIU, A. *Security Institutions as Agents of Socialization? NATO* in 'New Europe. *International Organization nr.59*, 2005.
9. GRIFFITHS, S. M., International relations, Schools, currents, thinkers, Bucharest, Publishing house: Ziua, 2003.
10. KATZENSTEIN, P. J., *The Culture of National Security: Norms and Identity in World Politics.* New York, Publishing house: Columbia University Press, 1996.
11. KEOHANE, R.O., NYE, J.S., *Power and Interdependence in International Organization*, Vol. 41, 2001.
12. SANÉ, P., *Rethinking Human Security*apud M. C. Goucha, *Rethinking Human Security* (pg. 5–6). Chichester, UKeditura Wiley-Blackwell Publishing, 2008.
13. SAVU, I. N., *Security studies*, Bucharest, Regional Center of Studies, 2005.
14. REUS-SMIT, C. *Constructivism" in Theories of International Relations, 2nd ed.* New York, Publishing house: Palgrave: Scott Burchill, 2001.
15. TADJBAKHSH, S., *Human Security: Concepts and Implications.* London, Publishing house: Routledge, 2007.
16. WÆVER, O. E., *Identity, Migration and the New Security Agenda* London, Publishing house: Printer, 1993.
17. WALT, S. M., *Renaissance of Security Studies, in International Studies Quarterly, Vol. 35*, 1991.
18. WENDT, A., Constructing International Politics. *International Security*, Vol. 20, 1995.
19. YU-TAI Tsai, "The emergence of human security: A constructivist view", *International Journal of Peace Studies*, Volume 14, No. 2, Autumn/Winter, 2009.

USEFUL TOOLS FOR MEASURING AND MONITORING CYBERSECURITY

Paula-Diana MANTEA, Ph.D.
National Intelligence Academy "Mihai Viteazul", Bucharest, Romania.
E-mail: mantea.paula@animv.eu

Abstract: *Cybersecurity is one of the new dimensions of security, the one responsible for ensuring a secure online space, a space which can be used safely in all areas of people's lives – from finance to social media, education, economy, politics, information, debate and even military. Because over 50% of the population is connected in 2020 to the internet, both for work and personal purposes, as numerous transactions are being registered in the cyberspace every second, government and private sector alike need to work together to secure this space to develop early-warning systems and protect the IT infrastructure of any kind of attacks. There are tools for measuring and monitoring cyber-attacks, which need to be explored and constantly improved. But this is not enough as the use of these tools needs to be completed by the joint efforts in raising the users' awareness in protecting against any attacks. Additionally, exploring and taking advantage of the benefits a digital economy and society can offer should be supported by investments in education and training while maintaining an updated and secure infrastructure.*

Keywords: *cybersecurity; indicator; monitoring; cyber-attack; cyber hygiene; education; awareness.*

Introduction – current state of cybersecurity

The current paper proposes an analysis of the current security context, in which cyber-attacks and IT&C security breaches are numerous and have an increasing impact both at a society level as well on the military dimension as numerous conflicts are being registered in the cyberspace between state and non-state actors. We will analyze and highlight the risks, threats, and vulnerabilities in the cybersecurity area.

We will look into the main available tools to measure cybersecurity at an international level and analyze Romania's position compared to other countries in terms of an important number of indicators used to assess this dimension of security such as overall legislation, technology, the existence of a cybersecurity strategy, level of capability development and cooperation in preventing, combating or responding to attacks in cyberspace, to increase cybersecurity resilience.

Technological innovations recorded in the last two decades, between 2000 and 2020, have affected all the activities we carry out in cyberspace in everyday life. But while we are witnessing the benefits that digital transformation is bringing on society by enabling global economic and social progress, at the same time cyberspace is facing numerous cyber-attacks and illicit use of technological resources.

1. Main cybersecurity risks, threats and vulnerabilities

Before analyzing the current situation of cyberspace incidents and alerts, it is interesting to note how it has developed over time. "The first major cyber-attack took place in

1988. Robert Morris created the first worm that targeted and infected about 6,000 devices, the equivalent to 10% of all internet-connected equipment at the time. To eliminate the infection, the administrators of the regional internet networks decided to disconnect them to neutralize the threat, taking action within a few days, during which time the entire existing internet network worldwide has ceased its activity"[1].

The complexity of cyber threats begins to increase after 2000, with the advent of Trojan applications, which allow attackers to hide their identity. These have been and are still in use today, as representatives of the leadership of the Cyberint Centre say, "both by actors in the field of cybercrime and by strategically motivated entities, since the first large-scale cyber espionage activities were initiated"[2].

Some representative examples of large scale espionage are APT – Advanced Persistent Threat actions – through which, groups of type APT1 – associated with a highly prolific group in China, or APT28 – SOFACY associated with the Russian Federation's Military Intelligence Service, GRU, "consisted in the exfiltration of information of strategic interest, which targeted both government and private targets"[3].

2010 was a defining year on the cybersecurity scene by identifying a new form of threat in cyberspace that of cyber sabotage. "Worm Stuxnet", known as an application, aimed at causing significant material damage, was designed to exploit zero-day vulnerabilities to illegally access critical infrastructure elements, such as equipment used to produce and enrich uranium.

This virus has affected Iran to the greatest extent, followed by Indonesia and India. Stuxnet differs from other similar attacks in the sense that it is of very high complexity, denoting highly advanced technical and digital skills, which very few hackers possess, and also requiring a significant number of resources. Although the entire cyber community is on constant alert following this attack, even riskier than the attacks on Estonia in 2007, there is a permanent alert in preventing such actions that endanger critical infrastructure, the implications it has had, and could have, exceeding any expectations.

The European Union Agency of Cybersecurity (ENISA) has elaborated the EU Threat Landscape Report for 2019 and first part of 2020 (April)[4], confirming last years' trend in which cyber-attacks develop into more sophisticated, targeted, widespread and usually undetected ones. The main motivation behind these attacks is still the financial one. In the last years it was observed that phishing, spam and targeted attacks in the social platforms were on an increasing trend. Malware, web-based and phishing attacks occupy the top 3 threats in the cyberspace in the specified time interval.

Moreover, statistics show that during the coronavirus pandemic there were numerous challenges on ensuring the cybersecurity of the health services, while the cyberspace changed at a general level because of the huge shift to teleworking, online learning and teleconferencing which needed to be prepared and enabled for numerous employees in a very short period of time, putting a high pressure on the IT divisions to cope with these evolutions in the cyberspace. In order to limit as much as possible, the impact and occurrence of cyber-attacks, we need to increase the cyber resilience. This implies having the capacity to resist to an attack or cyber incident, but also the capacity to recover fast and return to normal. Being

[1] Anton Rog, Cristian Condruț, *Evoluția amenințării cibernetice,* Romanian Intelligence Service, March 2019, URL: https://intelligence.sri.ro/evolutia-amenintarii-cibernetice/, accessed on October 1, 2019.
[2] *Ibidem*.
[3] ***, *Ghid de bune practici pentru securitate cibernetică,* Serviciul Român de Informații (SRI), p. 19, URL: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf, accessed on October 1, 2019.
[4] ***, *EU Threat Landscape Report,* URL: https://ec.europa.eu/digital-single-market/en/news/eu-threat-landscape-report-cyber-attacks-are-becoming-more-sophisticated-targeted-and, accessed on October 22, 2020.

more resilient implies also to increase cyber capabilities alongside with the awareness and education of the human resource, still the top target in the cyberspace.

2. Understanding cyber-attacks

To understand the impact of cyberspace attacks, we consider it important to review some definitions and main characteristics of terms used in cybersecurity field.

Thus, according to Romania's Cyber Security Strategy[5]:

- *security risk in cyberspace* is the likelihood of a threat materializing by exploiting a specific vulnerability specific to cyberinfrastructures;
- *cyber threat* is that circumstance or event that constitutes a potential threat to cybersecurity;
- *vulnerability* in cyberspace is a weakness in the design and implementation of cyberinfrastructures or in the related security measures that can be exploited by a threat.

According to the European cybersecurity rules which are transposed also in the strategic document in Romania, the types of threats in cyberspace include[6]:

- *cyber-attacks* against infrastructures supporting public utility functions or information society services whose interruption or impairment could constitute a threat to national security;
- *unauthorized access* to cyberinfrastructures, unauthorized *alteration*, *deletion* or *damage* to computer data or *unlawful restriction of access* to such data;
- *cyberespionage* (defined as "actions carried out in cyberspace to obtain unauthorized confidential information in the interest of a State");
- *property damage*, *harassment*, and *blackmail* of natural and legal persons, under public and private law.

According to the *ENISA Report on Cyber Attacks 2018*, we note that the main developments in cyberspace highlight that[7]:

- *phishing* actions occupy the first position within the main methods of infestation;
- *cyberspace operating kits* have lost their scale;
- *unauthorized cryptocurrency mining* activities have become an important source of hacker financing;
- *state-sponsored cyber-attacks on banks* are on the rise through the use of cybercrime attack vectors;
- due to the extremely large problems in filling vacancies in cyber field, one of the priorities of national actors in cybersecurity remains the *development of the set of technical and digital skills;*
- cyber-intelligence must combat the large number of *automated attacks* through innovative approaches precisely from the area of use of applications, tools, and automation skills;
- the development of the industry called the *Internet of Things* (IoT) remains an important concern due to the lack of mechanisms for the protection of lower-range IoT equipment and services. This remains a pressing need to create a universal architecture/good practice in the protection of IoT equipment and services;
- the absence of *cyberintelligence solutions* at the level of low-capacity organizations and end-consumers must be addressed and addressed by governments and producers.

When analyzing the global situation of cyber-attacks in 2018 compared to 2017, we observe that the top 4 threats remain the same, while ransomware attacks, insider attacks, and cyberespionage are decreasing. A notable feature in 2018 is that a third of attacks remained at

[5] ***, *Strategia de Securitate Cibernetică a României,* Guvernul României, 2013, pp. 7-8.
[6] ***, *ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends*, ENISA, January 2019, URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, accessed on October 2, 2019.
[7] *Ibidem*, p. 7.

the same level as the previous year. There is also a new type of attack in the top 15 in 2018 – unauthorized cryptocurrency mining – a new method of monetizing attacks on websites and apps.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	⊃	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	⊃	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	⊃	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure no. 1: Comparative analysis of the types of cyber-attacks recorded in 2017-2018[8]

As for the types of targets subject to cyber-attacks in 2018, according to the hackmageddon.com portal, their distribution ranks first: human resources, various industries, medical and public administration systems, the defense and social security field and financial activities as shown in the chart below.

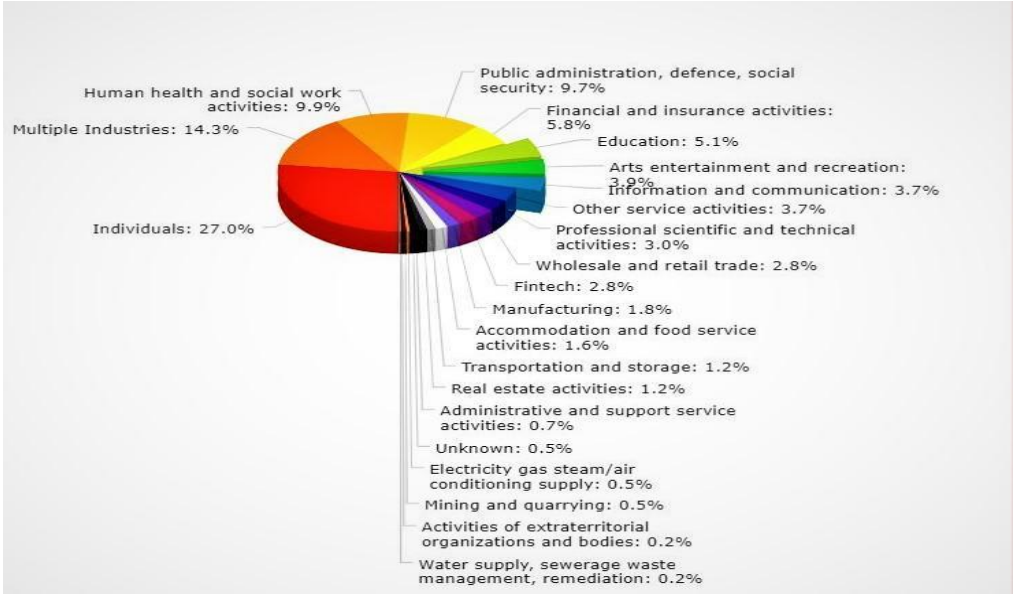


Figure no. 2: Distribution of cyber-attack targets in 2018[9]

[8] *Ibidem*, p. 9.
[9] Paolo Paseri, *2018: A Year of Cyber Attacks*, Hackmageddon, January 15, 2019, URL: https://www.hackmageddon.com/?s=Distribution+of+cyber-attack+targets+in+2018, accessed on October 14, 2020.

Compared to previous years, ENISA's analysis and reports on the evolutions and trends in cyberspace in 2019 and first quarter of 2020 indicate significant changes in the cyber threat landscape, mainly due to the covid-19 pandemic and the continuous trend in the advanced adversary capabilities of threat actors. Below we can observe the Top Threats Landscape Report for 2019-2020[10].

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking:** ↗ Going up, — Same, ↙ Going down

Figure no. 3: ENISA top threats 2019-2020

The main trends registered in 2019 and 2020 are: in the new stage of development of the digital transformation attacks are more and more numerous; the number of social and economic online transactions is reaching unthinkable levels and require huge data processing and storing capabilities; more and more attacks are registered in social media; state-sponsored actors sponsor attacks on high-value and sensitive data; credential theft is observed throughout the cyberspace at a global level; ransomware are still widely distributed and cause high financial loses to both state actors and organizations; a great cybersecurity weakness consists in the late detection of cybersecurity incidents; the human resource remains the greatest vulnerability in cyberspace due to the lack of cybersecurity awareness and training/education.

[10] ***, *EU Threat Landscape Report*, URL: https://ec.europa.eu/digital-single-market/en/news/eu-threat-landscape-report-cyber-attacks-are-becoming-more-sophisticated-targeted-and, accessed on October 23, 2020.

3. Tools for measuring and monitoring cybersecurity

Statistics say that over 50% percent of the global population is connected to the internet in 2020. This represents a step forward in the actions undertaken to globalize the information society into an inclusive one, but it also draws a wake-up call on the complexity and multitude of sources that need to be cyber-protected. The *ITU Connect 2030* analysis highlights the need to provide safe cyberspace, mainly due to estimates that more than 70% of the population will be connected to the Internet in the next decade (by 2030)[11].

Studies show that due to the increase in the use of IT&C technologies, it is expected that by the end of 2021 the estimated cost of global cybercrime will reach $6 trillion annually[12]. Although there have been fewer ransomware attacks, the number of security breaches related to personal data and critical infrastructure has increased, thus increasing the costs of maintaining safe cyberspace[13].

Besides that, there are differences between states in terms of how cybercrime legislation is implemented, national cybersecurity strategies provisions, Cyber Security Incident Response Teams (CERT), awareness and capacity to promote strategies, or cybersecurity capabilities and programs. Eliminating differences and ensuring a common standard of cyberspace security could ensure sustainable development in this area, together with increasing resilience and proper use of IT&C technologies and supporting economic growth.

The increase in cybersecurity incidents and breaches in recent years highlights the challenge faced by all internet users (governments, organizations, and citizens alike) in keeping up with developments in IT&C technologies, and cybersecurity must be part of this technological advance.

Ensuring cybersecurity is an ongoing process that must be able to counter cyber-threat activities and campaigns. In this respect, there is a need to develop and publish studies and reports on existing measurement indicators and the results they measure. These tools should be reviewed periodically to adapt to the need to respond to the continuous number of problems identified in the cyber environment especially by taking into account their cross-border nature.

3.1. Global Cybersecurity Index

Developed by ITU – the UN Agency specialized in Information and Communications Technology – this report analyses the level of states' commitment to combating cyber-attacks, but it also provides an overview of the cybersecurity situation in each state. The five pillars of the index are: legislation, technology, cybersecurity strategy, capability development, and cooperation.

Romania is in the middle of the ranking, occupying the 72nd position (out of 175) among the states with an average commitment. The report's conclusions reflect annual increases for the majority of respondents and encourage cooperation and communication. Education and training of experts in combating cyber-attacks are priority directions for action that decision-makers must follow.

---

[11] ***, *Global Cybersecurity Index 2018*, ITU, 2019, p. 6, URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, accessed on October 2, 2019.

[12] Steve Morgan, "Global Cybercrime Damages Predicted to reach $6 Trillion annually by 2021", *Cybercrime Magazine*, Northport, N.Y., December 7, 2018, URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, accessed on October 2, 2019.

[13] ***, Global Cybersecurity Index 2018, *doc. cit.*, p. 6.

Instruments developed by various competent cybersecurity bodies, including the Global Cyber Expertise Forum (GFCE), the Global Commission for Cyberspace Stability (GCSC), the Internet Governance Forum (IGF), the Commonwealth Telecommunications Organization (CTO) and the Global Cyber Security Capacity Centre (GCSCC) are made available to all stakeholders. ITU's recommendation is for government officials to take advantage of these opportunities by exploiting these available resources in identifying the most effective defense actions in the face of cyber-attacks.

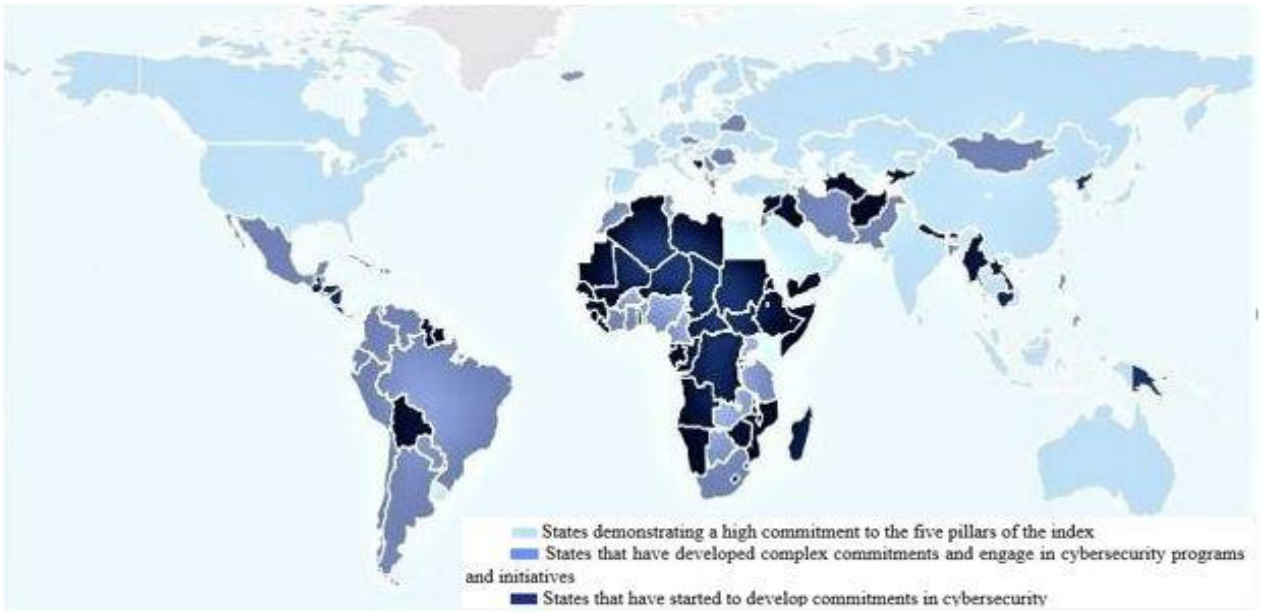


Figure no. 4: Map of national engagement in cybersecurity[14]

We can observe in the above map that most of the Northern Hemisphere states demonstrate a high commitment to the five pillars of the index in contrast with the Southern Hemisphere where states have only began to develop the commitments and started to engage in cybersecurity programs and initiatives. Considering the continuously increasing number of devices connected to the global internet network and the number of attacks and incidents registered annually, it emerges as crucial to invest in increasing cyber capabilities, in performance early warning systems, in adopting the right legislation and strategy to protect individuals and organizations against attacks and cooperating for ensuring a reliable and safe cyberspace. This map offers a nice insight in the current state of engagement and development of cybersecurity and it reveals that there are still many steps to follow to ensure the above mentioned common objective of ensuring a safe cyberspace – an objective for all actors present online, as cybersecurity represents a shared responsibility.

3.2. National Cybersecurity Index

It is an index developed by the *Estonian e-Government Academy* in cooperation with the Estonian Foreign Ministry. The index focuses on the public aspects of national cybersecurity that are implemented by the government administration. The purpose of this index is to measure the level of preparedness of states in the prevention, management and control of cyberspace threats and incidents. 100 states are part of this report which contains 46

[14] *Ibidem*, p. 13.

indicators from the virtual identity area, digital signature and the existence of a safe environment to develop online government services for citizens.

One advantage of this index is to be built on a global online database, which also indicates a number of recommendations that states can follow to improve their level of cybersecurity. It also provides an overview of how to manage attacks and cybercrimes, in parallel with the level of digitization of each of the 100 countries. The report on the 2017-2020 evolution positions Greece, Czech Republic and Estonia on the top of the list, with Romania ranked 21st. At the opposite pole we find Burundi, Tuvalu and South Sudan ranking last[15]. This tool is considered one of the most detailed cybersecurity indices in the world, which can be used to identify the areas of improvement at a country level. The portal is interactive, easy to use, it enables a function to compare entities and their evolution in the past three years. It is customizable and up to date and it is constantly refreshing the database.

3.3. Cyber policy portal

It is an online portal developed by the *United Nations Institute for Disarmament Research* (UNIDIR) in 2018 as a reference tool in the analysis of the state of cybersecurity and policies in the field. The portal was created to foster the active participation of all actors involved in key policy-making processes in cyberspace, to support information sharing, increased capabilities, trust and cooperation in cyberspace. The portal is based on public information available online and its advantage is that it has the ability to access information published in official documents at national or intergovernmental level in the original language.

3.4. Global Cyber Strategies Index

It is an index developed by the *Centre for Strategic and International Studies* (CSIS) as part of its technology program. The aim of this project is to facilitate a consolidated database of existing legal and global legal and frameworks for policymakers and diplomats to provide the necessary support and information to the global community in their efforts to understand, monitor and harmonize cyber regulations. The index includes references to national defense strategies in public and military cybersecurity, digital content, data privacy, critical infrastructure protection, e-commerce or cybercrime from public sources[16].

3.5. Other indicators measuring cybersecurity

There are also other relevant indicators and initiatives that measure the level of cybersecurity of companies or even companies providing cybersecurity advice to state and non-state actors, among which we list:

- Accenture – *Cyber Resilience Status*[17]
- Africa Cyber Immersion Center – *Report on Cyber Security in Africa*[18]
- Dell, Microsoft, IBM – *Cyber Security Index*
- *CyberGreen Cyber Security Index*
- *Kaspersky Cyber Security Index*

---

[15] ***, *National Cyber Security Index*, URL: https://ncsi.ega.ee/ncsi-index/, accessed on October 24, 2020.

[16] ***, *Global Cyber Strategies Index*, Center for Strategic and International Studies, URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/Cyber%20Regulation%20Index%20V2%20%28002%29.pdf, accessed on October 14, 2020.

[17] ***, *Cyber Resilient Business*, Accenture, URL: https://www.accenture.com/us-en/insights/cyber-security-index

[18] ***, *Africa Cybersecurity Report 2017. Demystifying Africa's Cyber Security Poverty Line*, The Africa Cyber Immmersion Centre, Serianu limited, 2018, URL: https://www.serianu.com/downloads/AfricaCyber SecurityReport 2017.pdf, accessed on October 14, 2020.

- *Index of the level of maturity of cybersecurity in Asia-Pacific*
- New York University – Tandon School of Engineering – *Cyber Security Index*
- NTT – *Report on Global Threats in Intelligence*
- Potomac Institute for Policy Studies – *Cyber Security Training Status Index 2.0*[19]
- Tenable Network Security & Cyber Edge Group – *Global Cyber Security Assurance Report*
- University of Oxford Global Cyber Security Capacity Centre (GCSCC) – *Cyber Security Maturity Level Index.*

Conclusions

According to the latest finalized public reports, we can conclude that 2018-2020 was a period with extremely complex activity in cyberspace, in which new forms of attacks have emerged, while others have faded. It has been a period in which important legislative steps have been taken in an attempt to unite the efforts of all actors involved in cyber-field and increase resilience to cyber-attacks globally.

The indicators which we consider relevant for measuring the level of cybersecurity are:

1. *Technology* – creating a standard framework of I&C technologies and security of information systems used in both the public and private sectors would reduce vulnerabilities in cyberspace and enable more efficient monitoring of networks, together with faster identification of security alerts. Eliminating the differences between technologies used in the digital economy and society and the proper use of information systems are indices of a more manageable cyberspace.

2. *Legislation* – the existence of a legislative framework to regulate activity in cyberspace is useful as long as it is applicable. Simply drafting and adopting legal acts and cybersecurity strategies are not enough. Clear methodologies for the implementation and evaluation of these legislative initiatives are needed to be able to establish effective bodies of expertise and response to cybersecurity alerts.

3. *Budget* – significant investments in cybersecurity are needed to allocate the financial, human and technological resources needed to develop a safe and resilient cyberspace in the face of attacks and incidents. In the absence of the correct prioritization of cybersecurity objectives and adequate financial support, it seems impossible to manage a secure cyberspace. The costs of training technical and cybersecurity experts, investment in the ongoing updating of IT&C technologies, research and the constant development of information systems, etc., are not at all small. So are the costs that security incidents cause annually. From this point of view, the budget needed to ensure cybersecurity should be important in discussions about annual budgets at both national and regional or global level, including at the level of economic actors or at individual level.

4. *Cooperation* – the creation of national or international cybersecurity incident response teams is an extremely important indicator for securing the online environment. The cross-border nature of cybercrime requires coordinated prevention, combat and response actions. Although there are many regional and global initiatives, there is no centralization.

[19] Melissa Hathaway et all, *Cyber Readiness Index 2.0. A plan for cyber readiness: a baseline and an index*, Potomac Institute for Policy Studies, November 2015, URL: https://www.potomacinstitute.org/images/CRIndex2.0.pdf, accessed on October 14, 2020.

BIBLIOGRAPHY:

1. ***, *ENISA Threat Landscape Report 2018. 15 Top Cyber threats and Trends*, ENISA, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
2. ***, *EU Threat Landscape Report*, ENISA, 2020, https://ec.europa.eu/digital-single-market/en/news/eu-threat-landscape-report-cyber-attacks-are-becoming-more-sophisticated-targeted-and
3. ***, *Global Cyber Strategies Index*, Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/Cyber%20Regulation%20Index%20V2%20%28002%29.pdf
4. ***, *Global Cybersecurity Index 2018*, ITU, 2019, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
5. ***, *National Cyber Security Index*, NCIS, 2020, https://ncsi.ega.ee/ncsi-index/
6. ***, *Romanian Cyber Security Strategy*, Romanian Government, 2013 *(In Romanian: Strategia de Securitate Cibernetică a României,* Guvernul României, 2013)
7. ***, *Cyber Green Stats*, Cyber Green, 2019. https://stats.cybergreen.net/country/romania/
8. *Cybercrime Magazine*, https://cybersecurityventures.com
9. Official website of Romanian Intelligence Service, www.sri.ro
10. Rog, Anton; Condruț, Rog, Cristian, Condruț. 2019. *Evoluția amenințării cibernetice.* March, 2019. https://intelligence.sri.ro/evolutia-amenintarii-cibernetice/
11. *Hackmageddon* website, https://www.hackmageddon.com

PHYSIOGNOMY OF INTERNATIONAL MILITARY OPERATIONS IN THE CURRENT OPERATIONAL ENVIRONMENT

Cosmina Andreea NECULCEA (SAGHIN)
Lieutenant, Ph.D. Student, Teaching Assistant, "Henri Coandă" Air Force Academy, Brașov, Romania. E-mail: saghincosmina@yahoo.com

Abstract*: In an ever-changing world, national security systems must recurrently adapt their capabilities to meet the new challenges of the international security environment. The way of approaching conflict and the physiognomy of military actions can be configured only through a thorough understanding of the current operational environment. Studies on demographic trends suggest that most future armed conflicts will take place in urban areas, whereas urbanization and unrestricted access to the Internet make the world become increasingly interconnected and interdependent.*

Keywords: *operational environment; key global trends; military operations on urban terrain (MOUT); cyber operations; adaptability; new threats.*

Introduction

The current security context is characterized by a series of challenges that are already manifesting or that "will manifest themselves through conventional and unconventional weapons, both in the military and the civilian environment and which will often be difficult to predict". [1] For an adequate answer to these challenges it is necessary the forecast which, according to the explanatory dictionary of the Romanian language, represents "the possibility to predict the appearance or evolution of future events or of some processes and systems (natural or social) based on the analysis of some currently known data". [2] The current security climate is uncertain, but this uncertainty is long-lasting, especially with regard to the ability to anticipate new forms of conflict.

The great American strategist Colin S. Gray claimed that "we knew nothing, with certainty, about the wars of the future, not even in the short term". [3] Therefore, studies on the future are not to predict the future but rather to improve the ability to cope with uncertainty, in other words, thinking "outside the box".[4] In an ever-changing world, national security systems must continually adapt their capabilities to meet new challenges of the international security environment. Even though there has been disapproval of the possibility of studying the future, "by not thinking about the future we succumb to the false idea that the world remains the same".[5] Defining future scenarios involves a prospective analysis, which stands for studying the past, knowing the present and researching trends.

While the physiognomy of conflicts is constantly altering, their nature remains intact because violence, chaos, uncertainty resulting from incomplete and unclear information

[1] *Romanian Armed Forces Doctrine*, p. 28.
[2] https://dexonline.ro/definitie/previziune, accessed on September 11, 2020.
[3] Colin S. Gray, *War: Continuity in Change, and Change in Continuity*, Parameters (Summer 2010), p.5.
[4] Editors Per M. Norheim-Martisen, Tore Nyhamar, *International Military Operations in the 21st Century. Global trends and the future of intervention*, Routledge, 2015, p.2.
[5] *Ibidem*, p.6.

continues to exist. The traditional border between peace and war has blurred. Therefore, finding an answer or identifying the final state of the conflict, using the classic terms of victory or defeat, is increasingly difficult. The rapid transformation of the morphology of wars forces us to anticipate their evolution, in order to be able to identify the most effective security measures to prevent and resolve crises.

Through this article, we aim to identify the characteristics of the current operational environment and to understand how global trends shape the international military operations.

1. The current operational environment - from the physical to the social environment

The current and future operational environment is characterized by instability and dynamism. This instability is the result of technological advance, human interaction and fluctuations in the economic and social environment. "A fundamental change in the operational environment parameter is the increased importance of knowledge of society, culture and attitudes, compared with importance of technical and material means".[6] The operational environment is a component part of the security environment, which has been transformed into a high-tech multi-domain battlefield. Therefore, in an attempt to transpose the approach to warfare beyond its traditional limits, the US introduces the term Multi-Domain Operations (MDO). Even though this term is used by the NATO and other nations, it is still undefined. So far, no unifying definition of multi-domain operations has been established because the NATO has not yet provided a definition for the term *domain*. However, within its Glossary of Terms and Definitions, the NATO offers a definition for the *operational environment*, which seem to be used interchangeably. Operational environment represents "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[7]

Through a thorough understanding of the operational environment, one can configure the way of approaching conflict and the physiognomy of military actions. Operational environment "includes land, seas, air and space, the enemy, neutral or other types of actors, infrastructure elements, weather forecast, terrain, electromagnetic spectrum, chemical, biological, radiological and nuclear/CBRN threats and dangers as well as the information environment".[8]

At the NATO Summit in Warsaw (2016), the Heads of State and Government participating in the North Atlantic Council meeting recognized Cyberspace as a Domain of Operations, with cyber defense becoming the central task of collective defense.

"Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea." [9]

The US military is recognized as the strongest in the world, but its opponents are making significant progress in Cyber Warfare to minimize the traditional dominance of the US in other areas. Basically, they use technological advances to create their own asymmetrical advantages. Therefore, to maintain this advantage, the US military, and not only, must maintain the ability to operate simultaneously in all areas.

The proliferation of technology leads to the idea that historical approaches to maintaining superiority in the air, on land and at sea may no longer be valid. These

[6] Kipp, Jacob, *The Human Terrain System: A CORDS for the 21st Century*, Military Review, 2006, p.12.
[7] AAP-06/Edition 2019, NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH), p. 93.
[8] ***, F.T.1 – Doctrine of Romanian Land Forces Operations, Bucharest, 2017, p. II-1.
[9] NATO, Warsaw Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, accessed 16 October 2020.

technological advances have also pushed the world into a realm where all previous notions of combat space have been radically modified.

A permanent assessment of the security environment is needed in order for one to be able to identify the evolutionary trends, the role and intention of the various actors as well as the risks and threats escalating manner.

Geographical factors refer to issues such as the strategic distance from the state contributing resources to a particular area of operations and accessibility in that area. Long distances involve significant costs and the existence of strategic transport capabilities, while the accessibility of the area requires the existence of a minimal infrastructure the existence of Host Nation Support (HNS) and enemy's presence in that area. In terms of infrastructure, the most common operations take place in countries with poor infrastructure or little HNS. Therefore, one of the objectives of military operations is to build and protect this infrastructure. Some peculiarities of the terrain may favor the regular forces, while others are in favor of the irregular ones. For example, plain or desert areas benefit from conventional forces, whereas mountain areas provide shelter for insurgents, temporarily allowing them to retreat.

The conduct of military operations can also be influenced by the climate factor. Soldiers coming from various parts of the world will find it very difficult to adjust to the climate of a particular area of operations. In addition to the need for climate adaptation, tropical diseases are also a real problem. At the same time, the climate also affects military equipment, technology, weapons. Climate change affects health, economy and landscape and can lead to loss of life, famine, diseases.

Generally speaking, population, culture and local norms are components of the operational environment, as well. In modern operations it is essential to know the culture and written norms or unwritten customs of a certain area. An offensive behavior of international forces towards norms or policies could induce a negative attitude of rejection in the population. It is also crucial to know the socio-economic conditions of society. Improper use of economic and social means can generate tensions, which often lead to new conflicts. All these aspects, of a physical and social nature, represent an important part of the current operational environment.

In order to guarantee the success of the operations, it is imperative to know these aspects before the operation starts. The war could become less and less structured and operations could no longer be conducted in clearly defined areas. Therefore, a reassessment of the approach to future confrontations is needed, providing that past and current considerations are not neglected. However, these approaches will have to be adjusted in order to face the new faces of the adversary.

2. Key global trends – how they shape international military operations in the future

The management of international military operations, are determined by a series of key factors, among which we mention: demographic and environmental changes, economic trends, technological trends, new conflicts, actors and missions.

The first factor that may directly or indirectly affect the conduct of international military operations is the *demographic and environmental change*. The latest demographic data shows that the world will face a significant increase in population, *The New Population Bomb (Goldstone; 2010).* "The world population is projected to reach 9.9 billion by 2050, an increase of more than 25% from the current 2020 population of 7.8 billion".[10] Also, the aging

[10] https://www.prb.org/2020-world-population-data-sheet/, accessed on September 10, 2020.

population will affect the resilience of states in front of future crises. In addition to population growth and aging, there is another trend today, the urbanization of society. The three demographic trends can lead to a lack of management (control) which can favor the emergence of terrorist groups, organized crime organizations, extremist groups, etc. Therefore, urban agglomerations are prone to crime and violence. Once military operations move to urbanized areas, they will require the adoption of specific doctrines, tactics, equipment, etc.

Demographic changes are also affecting *the economy*. The costs of deploying and supporting large bases and military troops in theaters of operations are significant. Therefore, future military operations will involve the deployment of small number of troops (using Special Forces) or training and educating "indigenous forces"[11]. It is clear that stabilization operations, carried out by host nation forces, can even increase the operational effect.

The impact of new technologies significantly changes the way military operations are conducted. Technological advance has undergone a spectacular evolution, spreading to fields such as nanotechnology, biotechnology or other new ones. The world is becoming increasingly dependent on information and technology. Access to information is unrestricted but the infrastructure becomes vulnerable. Therefore, "understanding how people might use technology will be more important than the technology itself". [12]

The three factors analyzed above contribute to emphasizing the difference between developed and developing countries, only. Without a clear delimitation between the actions of *state and non-state actors*, as well as the use of all means, conventional/unconventional, it is possible to appear "an amalgam of threats, stimulated by accidental or uncoordinated actors, or hybrid threats".[13] In this sense, the germs of the new conflicts could be: inequality between states, limited access to natural resources, competition for coal, steel and other minerals, etc. Mobile phones can also be a real threat, being the fastest and most efficient means of mass mobilization.

The early identification of trends that will shape future military operations can help states adapt, anticipate, and respond appropriately to the security challenges posed by a constantly changing world.

3. Types of missions relevant to international military operations

Regardless of changes in global security and the nature of the conflict, the absolute priority will be the protection of people, irrespective of their nationality. In most operations, the protection of civilians has become a strategic necessity, given that civilians have become a highly sought-after target. In the contemporary operational environment, a wide range of missions take place, among which we mention: high-intensity operations, counter-insurgency operations, military advising and assistance operations, special forces operations, UN operations, etc.

Given the characteristics of the current operational environment and the evolutionary trends identified and described above, the future armed conflict may be characterized by[14]:

---

[11] Multiple Future Project, *Navigating toward 2030, final report* – april 2009, p. 9. https://www.act.nato.int/images/stories/events/2009/mfp/20090503_MFP_finalrep.pdf, accessed on September 10, 2020.

[12] Editors Per M. Norheim-Martisen, Tore Nyhamar, *International Military Operations in the 21st Century. Global trends and the future of intervention*, Routledge, 2015, p.13.

[13] *Ibidem*, p. 33.

[14] NATO, *Report/Framework For Future Alliance Operations, Nato Unclassified - Publicly Disclosed*, 2018, p.13, https://www.act.nato.int/images/stories/media/doclibrary/180514_ ffao18.pdf, accessed on September 10, 2020.

a. more interconnectivity across the recognized domains of warfare (air, land, sea, cyberspace), as well as space and the information environment (e.g., social media);
b. operations in the cyberspace domain, global commons (areas outside jurisdiction of any one nation), densely populated, and subterranean areas.

Studies on demographic trends also suggest that most future armed conflicts will take place in urban areas. But with urbanization and technological developments, the world is becoming more and more interconnected. Therefore, we conclude that the new physiognomy of international military operations will bear the image of at least two types of operations, urban operations and cyber operation.

3.1. Military Operations on Urban Terrain

Urban areas are constantly evolving due to population growth and migration from poor to developed areas, especially urban ones. Paraphrasing David Kilcullen (2013), future conflicts will move "out of the mountains, and into the cities." [15] The urban environment includes centers of industry, commerce and social activities that provide people with jobs, basic resources and other facilities. Due to the large number of inhabitants, urban areas will be a source of insecurity, as they integrate different groups from a cultural, ethnic, social point of view, groups that live in various conditions and whose perception of their role in the community differs. The physical and social complexity of these areas is a real challenge for the military forces, which will have to perform tasks such as community policing, disaster management, combat operations, etc. *The presence of significant numbers of non-combatants remains one of the defining characteristics of operations in an urban area.* [16]

In the armed conflicts of the last century, cities have played an important role, analyzed mainly in political terms. Also, in most conflicts, cities have been real strategic objectives, but difficult to conquer. The deployment of military operations in urban areas was devastating and costly. For example, the conventional Second World War (WWII) combat operations in urban areas are clear evidence that they were very demanding, because the fighting took place *on*, *over* and *underground*. [17] Moreover, "cities in the East and subsequently also in the West gradually became fully fledged targets and the theaters of decisive battles"[18], like Stalingrad, Budapest, Berlin, Amsterdam, etc. However, new urban operations are not as traditional. Conventional operations that involved the destruction of a certain area, in its entirety, become useless, because the new operations will pursue the selective destruction of certain targets or areas and, for a decisive effect, will not only disrupt the physical resources of the enemy but also attack the source of its power, of its will to fight.

Urban areas create conditions of uncertainty and chaos, being directly influenced by social development. Population density also includes the density of all types of media (newspapers, televisions, social networks).

Therefore, the main goal will be to influence public perceptions and consciousness through information campaign. *The attitude of the local population, whether hostile, compliant or supportive, will be an important factor in planning an appropriately scaled and*

[15] Kilcullen, David, *Out of the mountains. The Coming Age of Urban Guerilla*, New York: Oxford University Press, 2013.
[16] Report by the RTO Studies, Analysis and Simulation Panel Study Group SAS-030, *Urban Operations in the Year 2020,* RESEARCH AND TECHNOLOGY ORGANISATION, April 2003, p. 7, https://apps.dtic.mil/dtic/tr/fulltext/u2/a413638.pdf, accessed on September 12, 2020.
[17] Editors Per M. Norheim-Martisen, Tore Nyhamar, *International Military Operations in the 21st Century. Global trends and the future of intervention*, Routledge, 2015, p.137.
[18] Vautravers, Alexandre, *Military Operations in Urban Areas*. International Review of Red Cross, Volume 92, Number 878, June 2010, p. 439.

resourced force structure. [19] The image of insurgency and counter-insurgency has also become urban. In this type of environment, insurgents can adopt asymmetric methods faster and more efficiently without exposing themselves much and can take advantage of the weakness of counter-insurgency forces to operate in this type of environment.

Guerrillas, insurgents and other non-state groups have all taken advantage of the benefits (to them) of operating in such an environment and will no doubt continue to do so. [20] (for example Belfast, Mogadishu and Bogota). The forces that will operate in the urban environment will have to have the capacity to act in the proximity of an enemy familiar with the terrain, and the maneuvering approach, in this case, will be a difficult one.

Military commanders will have to adapt their organization of forces, command and control, as well their training, to deal with new threats. In the future, these operations will be inevitable, complex and difficult to manage. An important role will be played by the Rules of Engagement (ROE), as well as the observance of the chain of command, which will have to be considered before the operation starts. *While traditional warfare will continue, rules of engagement and the laws of armed conflict will increasingly become less clear.* [21] At the same time, information operations will directly affect the development of future operations and will play a crucial role.

The destructive effects of military operations in the urban environment can be avoided only by adapting doctrines and capabilities to the new reality.

3.2. Cyber operations

The concept of Cyber Warfare was first used in 1993, when two researchers from the U.S. RAND Corp publish an article entitled *The cyberwar is coming!*[22], emphasizing the role of battlefield information systems and the impact their disruption would have. Even though it has been recognized as a new field of confrontation, it cannot be admitted that future military operations can only take place in the cyber space, the nature of the conflict remaining the same. A future war will also have a cyber component (from espionage via information operations to attacks on the enemy's vital electronic systems).

"The cyber domain is defined as the physical and logical interconnection of information systems, including network devices, communications infrastructure, media and data".[23] By design, the cyber domain has no boundaries and is not characterized by geographical aspects.

"Cyber operations can be characterized as applying political pressure without resorting to physical attacks and infringement of another state's territory". [24]

For example, in 2007, Estonian authorities decided to move the Bronze Soldier (the Soviet WW II memorial in Tallinn) to the outskirts of the city, near a cemetery. This operation was seen by Moscow as a defamation of fallen soldiers buried nearby. Tensions turned into two nights of riots between Russian ethnic groups and an Estonian nationalist

[19] Report by the RTO Studies, Analysis and Simulation Panel Study Group SAS-030, *Urban Operations in the Year 2020*, RESEARCH AND TECHNOLOGY ORGANISATION, April 2003, p. 7, https://apps.dtic.mil/dtic/tr/fulltext/u2/a413638.pdf, accessed on September 10, 2020.
[20] *Ibidem*, p. 5.
[21] Sloan, Stefhen, The Challenge of Nonterritorial and Virtual Conflicts: Rethinking Counterinsurgency and Counterterrorism, JOINT SPECIAL OPERATIONS UNIVERSITY, 2011, p. 12.
[22] Arguilla, John, Ronfeldt, David, *Cyberwar is coming!*, COMPARATIVE STRATEGY, Vol.12, No.2, 1993, pp. 141-165.
[23] Editors Per M. Norheim-Martisen, Tore Nyhamar, *International Military Operations in the 21st Century. Global trends and the future of intervention*, Routledge, 2015, p.175.
[24] Diesen, Sverre, *Cyber operations – Game Changer or Supporting Activity?* Presentation at Norwegian Armed Forces Cyber Defence's Cyber Conference, 18 April 2013.

group. A series of cyber attacks followed, and the Estonian state claimed that these attacks were initiated from the Russian territory. However, the Russian government denied any involvement in the cyber attack and refused to assist Estonia in identifying computers on the Russian territory. These attacks have been listed as the first cases of cyber warfare (Estonia: Attacks Seen as First Case of 'Cyber War'[25]).

Another example would be the conflict between Georgia and Russia or the war in Afghanistan in which, in addition to conventional military means, the cyber attack was also used. The potential of Cyber War was illuminated by Russo-Georgian conflict and determined Pentagon *to formally designate cyberspace as a* "warfighting domain". [26]

This incident had a major impact on the operational environment and prompted NATO to protect itself and respond against such attacks. Knowledge of operating systems as well as specific configurations are required to conduct cyber attacks. In most cases, before executing a cyber attack, it is necessary to build an exact copy of the adversary's system, in order to perform extensive tests. Once these systems are used, the adversary will identify vulnerabilities and ensure that this weapon will not be used again. Not least, "to be successful in using cyber means as part of an advanced military operation, one would also need a large and highly developed intelligence organization." (Diesen; 2013).

Cyberspace is the only domain created entirely by man which is constantly changing in response to technological innovations.

Failure in one area can cause cascading effects in other areas. It is not excluded that Cyber Warfare conducted in the cyber space will produce kinetic effects or any other effects outside the cybernetic domain. For example, the attacker can target people whose lives depend on computer systems (means of transport, different kinds of medical, professional or military life-support system). Also, all devices that use cyberspace can be targets or real threats. The cyber space is an option for both friendly, neutral or enemy forces.

Nowadays, we see "virtual theaters" that "draw in populations and forces with no geographical connection to the conflict and which may be located anywhere on the planet". [27] Therefore, despite the physical distance, the population and forces deployed at a distance from the area of operations, may conduct offensive cyber operations. An important aspect is represented by cyber dependencies across borders and the distinction between military and civilians makes it difficult to separate society from the conflict zone. Interoperability is a key feature to operate efficiently with allies and lead successful operations.

In the future, it will be difficult to identify a military operation without the implication of cyber domain. "Superiority in the physical domains in no small part depends on superiority in cyberspace".[28] A new challenge would be to find an answer to the question: "Who is the puppeteer in the often impenetrable clouds of cyberspace?" [29]

[25] https://www.rferl.org/a/1076805.html, accessed on September 10, 2020.
[26] https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/, accessed on September 10, 2020.
[27] Kilcullen, David, *Out of the mountains. The Coming Age of Urban Guerilla*, New York: Oxford University Press, 2013, p. 172.
[28] https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM23-Mar-18.pdf, p. 2, accessed on September 10, 2020.
[29] Sloan, Stefhen, *The Challenge of Nonterritorial and Virtual Conflicts: Rethinking Counterinsurgency and Counterterrorism*, JOINT SPECIAL OPERATIONS UNIVERSITY, 2011, p. 17.

Conclusions

For the international military forces, the presence of new actors on the global battlefield is a real challenge. The nature of the adversary is complex and often clandestine. The adversary can use the most sophisticated technology, which leads to the need to adapt forces to new types of threats.

In a globalized world, with unrestricted access to the Internet, it is vital to think "*outside the box".* Therefore, it is necessary to adapt the military forces according to the nature of the opponent and the methods used by it. For those who need to plan and operate in the non-territorial space, it is vital to move out of their comfort zone. The new generations of politicians, military leaders, and strategists will have to develop this ability to think, plan and act non-territorially.

Awareness of the transformations in the security environment and the complexity of the operational environment of future conflicts will require the adaptation of doctrines, concepts and military forces to be able to carry out missions in these environments, urban and cybernetic.

BIBLIOGRAPHY:

1. *** AAP-06/Edition 2019, NATO Glossary of Terms and Definitions
2. *** NATO, Warsaw Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm
3. *** Presidential Administration, National Defence Strategy for the Period 2020-2024. "*Together, for a safe and prosperous Romania in a world marked by new challenges*", Bucharest, 2020.
4. *** Romanian Military Doctrine, Bucharest, 2012.
5. ***, F.T.1 – Doctrine of Romanian Land Forces Operations, Bucharest, 2017
6. ARGUILLA, John, RONFELDT, David, *Cyberwar is coming!*, Comparative Strategy, Vol.12, No.2, 1993.
7. COLIN S. Gray, *War: Continuity in Change, and Change in Continuity*, Parameters (Summer 2010).
8. DIESEN, Sverre, *Cyber operations – Game Changer or Supporting Activity?* Presentation at Norwegian Armed Forces Cyber Defence's Cyber Conference.
9. GOLDSTONE, J.A. (2010). "*The new population bomb*", Foreign Affairs 89 (1).
10. KILCULLEN, David, Out of the mountains. The Coming Age of Urban Guerilla. New York: Oxford University Press.
11. KIPP, Jacob, The Human Terrain System: A Cords for the 21st Century, Military Review, 2006.
12. PER M. Norheim-Martisen, Tore Nyhamar, *International Military Operations in the 21st Century. Global trends and the future of intervention*, Routledge, 2015.
13. SLOAN, Stefhen, *The Challenge of Nonterritorial and Virtual Conflicts: Rethinking Counterinsurgency and Counterterrorism*, Joint Special Operations University, 2011.
14. VAUTRAVERS, Alexandre, *Military Operations in Urban Areas*. International Review of Red Cross, Volume 92, Number 878, June 2010.

THE IMPORTANCE OF TRAINING IN THE SECURITY AND DEFENCE. WHAT IS MISSING IN THE ROMANIAN CSDP RELATED TRAINING?

Ovidiu Laurian SIMINA, Ph.D.
PhD in Economics, Head of Training Civilian Deployable Capability (CDC Romania) and Senior Research Fellow Timișoara Centre for Migration and Mobility Studies – SISCE.
E-mail: ovidiu.simina@cdc-romania.eu

Bogdan MARINESCU, Ph.D.
PhD in Sociology, Associate Professor University of Pitești and National College of Home Affairs, "Alexandru Ioan Cuza" Police Academy; Bucharest, Romania.
E-mail: bogdan.marinescu@cdc-romania.eu

Grigore SILAȘI, Ph.D.
PhD in Economy, West University of Timișoara, Emeritus Professor, Jean Monnet Professor, and Timișoara Centre for Migration and Mobility Studies – SISCE, Director, Romania.
E-mail: grigore.silasi@migratie.ro

Abstract*: The paper discusses the importance of training for the success of Romania's contribution to the Common Security and Defence Policy (CSDP) of the European Union. At the time when the EU Member States are taking concrete measures to implement the European Compact for a Civilian CSDP (2018) and the second annual progress report is planned, Romania is still struggling with the inter-institutional negotiation of the would-to-be National Strategy for the Implementation of the Civilian CSDP Compact, not yet approved by the Government. However, training is not seen as a strong point in the future strategic document, probably because there is not real coordination in the field. Despite the increased interest in CSDP related training (the number of the Romanian members of the European Security and Defence College multiplied five times in just two years), the training institutes are not working in a coordinated way and most of their CSDP training seems mostly related to individual projects or targets and not following a national policy, nor national objectives related to the Civilian Compact implementation. The debate opened by this paper aims to increase the awareness at the national authorities' level and to suggest the way ahead in liking training to the Romanian policy on CSDP.*

Keywords*: European Union; security and defence; crisis management; CFSP/CSDP; civilian capability development; training; Romania; Civilian Compact.*

In its attempt to become a global actor, influencing the world and projecting vision, interest and power, the European Union (EU) acts based on an external policy designed by the Member States, the Common Foreign Security Policy (CFSP). This policy aims to strengthen the EU's external ability to act in defending and promoting the Union's core values and principles during external crisis situations which, in certain ways, may impact the territory, people or the interests, as well as the internal security, of the EU or of its Member States. The EU acts externally considering the international law, human rights, rule of law or the democratic principles. Considering the increased complex and uncertain security environment

and the various crisis over the globe, the EU aims to become more capable, coherent and to act more strategic[1]. The Union has an integrated (comprehensive) approach towards crisis: when crisis occur, the EU is able to employ all instruments available in its crisis management toolbox, such as diplomacy, conflict prevention, peacebuilding and mediation, sanctions, security, defence, financial, trade, development cooperation or humanitarian aid (the EU is the world's largest trading block and, collectively, the world's biggest donor of official development assistance and humanitarian aid)[2]. To be able to respond to and engage with different types of external crisis, the EU has gradually developed an institutional framework, a decision-making process and a series of tools and mechanisms, placing the main emphasis on the capacity development (civilian and military capabilities in conflict prevention and crisis management).

Part of the CFSP, the Common Security and Defence Policy (CSDP) enables the Union to have a role in peace-keeping operations, conflict prevention and in the strengthening of the international security. *The most visible EU commitments to international peace and security remain its missions and operations deployed outside the Union*[3]. Under the framework of the CSDP, the EU has undertaken many operations outside its external borders, using civilian and military instruments: some 37 missions and operations have been launched since 2003, with the aim of bringing stability, rule of law, and security sector reform or to monitor crisis and peace agreements in countries as diverse as Bosnia and Herzegovina, Afghanistan, Georgia, the Democratic Republic of Congo, Ukraine or Iraq. Out of them, 17 missions and operations are still active on three continents (Europe, Africa and Asia), representing 6 military missions and operations and 11 civilian missions[4].

Civilian and military capabilities are at the core of every EU CSDP mission and operation, hence adequate and sufficient capabilities are the prerequisite for the successful mission's mandate delivery and the implementation of the assigned tasks in the field. Building capabilities ready for being used in crisis management environment requests investments, mainly investment in people. As having committed themselves to a CFSP/CSDP, the Member States are supposed to implement the needed measures in order to achieve the desired outcome. Equipping the people to be deployed with the necessary set of knowledge, skills and competences for performing their tasks in often challenging conditions, lies on the Member State *duty of care*. Training of staff is paramount for the successful of any action or activity, and especially for the success of the CSDP missions and operations.

"The nature of crisis management is increasingly evolving as CSDP missions and operations are tasked to carry out a diversified array of activities. This entails a strengthened investment in ***quality human resources****, hence an enhanced need to ensure that staff deployed is adequately equipped,* ***possesses the necessary knowledge, skills, and attitudes*** *required to*

---

[1] *When EU officials or scholars use the term 'crisis', there is a good chance they are referring to an international conflict, a large-scale disaster, or a failed non-EU state* (EUNPACK 2016: 5).

[2] Joint Communication to the European Parliament and the Council, *'The EU's comprehensive approach to external conflict and crises'*, JOIN/2013/030 final, URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52013JC0030

[3] Tania Lațici, *The Civilian CSDP Compact. A stronger EU footprint in a connected, complex, contested world*, European Parliamentary Research Service, Members' Research Service, PE 630.295, March 2019.

[4] N.A.: Currently, the following CSDP missions and operations are ongoing: ALTHEA/BiH, EU NAVFOR Somalia, EUAM Iraq, EUAM RCA (the newest CSDP mission in Central African Republic has been established on 9 December 2019 and become operational on 9 August 2020), EUAM Ukraine, EUBAM Libya, EUBAM Rafah, EUCAP Somalia, EUCAP Sahel Mali, EUCAP Sahel Niger, EULEX Kosovo, EUMM Georgia, EUNAVFOR MED IRINI, EUPOL COPPS/Palestinian Territories, EUTM RCA, EUTM Somalia, EUTM-Mali. An EU Commission instrument, EUBAM Moldova and Ukraine is not managed within the CSDP structures, but its objectives are similar with the other missions. For more details, see URL: https://eeas.europa.eu/topics/security-defence-crisis-response/430/military-and-civilian-missions-and-operations_en

*perform assigned duties, enjoys an adequate level of "protection" by the sending organization/State in the exercise of its duty of care vis-à-vis deployed personnel. Also, the involvement of other actors in crisis management, requests coordinated efforts for ensuring understanding and compatibility of approaches to work between organizations. In this regard, several fundamental aspects related to recruitment, **training**, contractual status of personnel of CSDP missions and operations are to be considered."*[5]

In order to achieve the level of ambition regarding the external action, the EU has encouraged the dialogue between its members on the CSDP capability development, various initiatives aiming to help (and push) Member States to address the persistent capability shortfalls through concrete actions. "Comprehensiveness refers not only to the joined-up deployment of EU instruments and resources but also to the shared responsibility of EU-level actors and member states"[6]. The states have been encouraged to adopt and implement national strategies to foster national capacity building for CSDP missions, to establish national budget lines for civilian crisis management and to share best practices. And to reenforce the training programme they are supposed to deliver as part of *duty of care*.

1. CSDP training environment at EU level

Over time, ambition, scope and range of the EU's missions and operations evolved and the CSDP continues to develop as an integral part of the CFSP, providing the EU with the means to act effectively became extremely important. To be effective in the implementation of their mandate granted by the Council of the European Union, the CSDP missions should have the ability to employ the right people with the right skill sets in the right place at the right time. CSDP missions and operations are generally deployed to places associated with elevated risks for the staff. Training and deployment are interconnected: if not trained properly, the staff may be a liability to themselves or others.

With the adoption of the EU Policy on Training for CSDP on 3 April 2017, *appropriate training has become a prerequisite for deployment for all staff*, including seconded and contracted personnel. CSDP training is recognised as being part of the global training architecture. The CSDP training must respect the strategic guidelines laid down by the European Council and the conclusions setting the direction of CSDP, while following the direction defined in the EU Global Strategy with its emphasis on a rules-based global order.

"To ensure its relevance, training must rigorously reflect EU policy, as elaborated by the Council, whether geographical or thematic, such as the EU Global Strategy on Security and Defence, the EU-wide strategic framework supporting Security Sector Reform, and the EU's 'Strategic Framework and Action Plan on Human Rights and Democracy'. It is also important that it be coherent and consistent with the external aspects of other EU policies, the work of the European Commission and that of Member States."[7]

Regarding training and general duty of care, EU bodies, Member States and CSDP missions and operations have shared responsibilities. The Member States deploying people to CSDP missions and operations bear the obligation of training own staff before the deployment (basic/core, advanced and pre-deployment training). Each Member State maintains the decision on organising own training system, but "in order to support the training activities provided by Member States, and to facilitate and complement them, the EEAS

[5] *Civilian and military personnel in CSDP missions and operations*, European Parliament, Directorate-General for External Policies, Policy Department, EP/EXPO/B/SEDE/2016/02, February 2017, DOI:10.2861/354308.
[6] Joint Communication to the European Parliament and the Council, *'The EU's comprehensive approach to external conflict and crises', op.cit.*
[7] *EU Policy on Training for CSDP*, 7838/17, 3 April 2017, Council of the European Union, para. 10.

provides basic guidelines and performance standards, descriptive materials and procedures covering the training cycle"[8]. The crisis management structures under the European External Action Service (EEAS) in Brussels run training needs analysis and define training requirements (training for CSDP should be driven by needs and requirements, not by events), and also look into the implementation of the lessons learned derived from CSDP missions and operations and at their implication on training[9].

The *Civilian CSDP Compact* of 2018 also links the deployment of personnel to the capacity building at national level, training included by default. Generic and core training should be provided as part of the general preparation of all staff envisaging working in the CSDP environment, while the advanced training is dedicated to experts targeting specific positions in CSDP missions and operations (such as Rule of Law, Security Sector Reform, gender mainstreaming, strategic communications or strategic planning and command of CSDP missions and operations). Personnel deploying to high risks area shall follow HEAT (Hostile Environment Awareness Training, which is mandatory before deployment to specific mission areas[10], together with the on-line courses BASE and SAFE made available by the EEAS on its website[11]). At the same time, all staff recruited for CSDP missions shall receive certificated pre-deployment training as a prerequisite prior to deployment. This training is aimed to complement the general training provided by the state of origin, and other types of training offered in the wider area of CSDP related training (see Figure no.1).

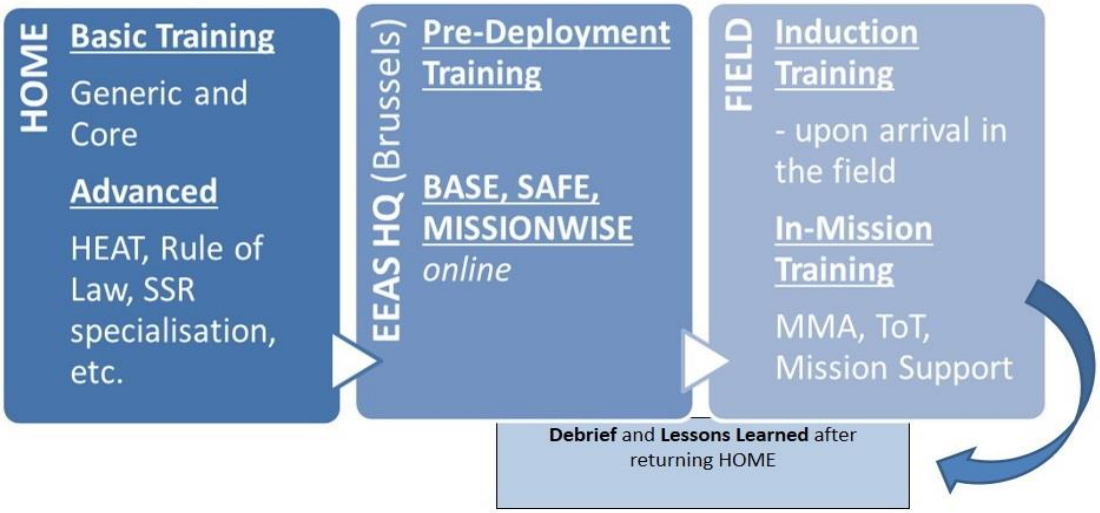


Figure no. 1: CSDP Training Cycle[12] (and duty of care): Shared Responsibilities

As having direct employment connection with the contracted staff, the Missions are responsible for their pre-deployment training. Along with the induction training, meant to familiarise the newly deployed (seconded or contracted) personnel with the realities of the

[8] *Ibidem*, para. 29.
[9] A.N.: As a contribution to operational effectiveness, the training architecture provides an agreed framework for all stakeholders, defines different types of training and the CSDP training audience and fosters alignment in training standards and methodologies. The lessons identified from CSDP missions, operations and exercises – as well as related activities – are systematically implemented in training so it supports the mission.
[10] A.N.: The HEAT course enhances the effectiveness of CSDP missions and operations by building on the safety and security skills of the mission personnel, also promoting increased safety and security awareness and developing self-confidence in a hostile environment.
[11] EEAS, Security eLearning, URL: https://webgate.ec.europa.eu/eeas/security-e-learnings/
[12] Based on *Figure 18: Training Cycle and Duty of Care: Shared Responsibilities*, GAREA 2019-2020, Annex VI, p. 75.

Mission's area of operations and the specificities of the work, the CSDP missions and operations may also equip own staff with upgraded knowledge on mentoring, monitoring and advising, train the trainers, logistic support or, as appropriate, HEAT training of the contracted staff. In-mission training, provided upon the arrival in the field, offers a cost-effective option since expenses arise only for trainers and the blended training could also make use of the on-the-job learning and mentoring approach.

However, as pre-deployment training is instrumental to the maintenance of a common organisational standard for all personnel and assists in developing a common organisational culture, a unique pre-deployment training programme has been established at the HQ level in Brussels. And both Member States and the CSDP missions and operations are encouraged to send their staff to follow the Brussels based pre-deployment training offered on monthly basis by the European Security and Defence College (ESDC). The ESDC uses a standard curriculum elaborated in the framework of the working group on CSDP missions and operations training[13] and approved by the 28 Member States (UK included).

The main CSDP training actor at EU level, included in the crisis management structures, hence embedded in the EEAS but with own legal capacity, the "ESDC shall provide training and education in the field of CSDP at the EU level, in order to develop and promote a culture of excellence, a common understanding of CSDP among civilian and military personnel and to identify and disseminate, through its training activities, best practice in relation to various CSDP issues"[14]. An independent sui-generis organisation and a "network College", the ESDC is organised as a network bringing together civilian and military institutes, colleges, academies, universities, training centres and other actors dealing with security and defence policy issues within the Union, as identified by Member States. The ESDC is the only EU training actor with a civil-military and integrated approach, covering the entire spectre of CSDP training and education, from basic courses to advanced training and leadership. The ESDC activity is basically relying on the training provided by the various network members and included in the ESDC training programme. Supporting the CSDP missions and operations falls among the ESDC main objectives (see Box no.1).

Standardisation of the training activities represents one of the most important features of the ESDC, other than providing standard courses together with training actors from the Member States and hence offering the members the framework for dissemination of their strategic messages and views on CSDP[15]. All network members running courses as part of the ESDC training calendar should follow the ESDC training approach and observe certain rules. They use the standard curricula approved for a certain training, and the evaluation report of al training activities shall be presented for analyse in the framework of the ESDC Executive Academic Board (EAB), before being endorsed by the ESDC Steering Committee (comprising representatives of all EU Member States).

ESDC uses the annual academic cycle, as most of the network members are part of national education systems: the academic year starts on 1 September and ends on 31 August the next calendar year. The annual training cycle (curricula development included) at the ESDC starts with the EAB meeting in September. The representatives of the network members gather in Brussels (or they connect online, as recently happened in the current

[13] A.N.: A project oriented configuration of the Executive Academic Board of the ESDC, the working group contributes to the co-ordination, coherence and quality of training personnel for CSDP missions and operations and to assist in creating a better link between the personnel to be deployed or serving in missions and the EU crisis management structures. More details could be found at URL: https://esdc.europa.eu/working-group-on-csdp-missions-and-operations-training-wg-mot/

[14] *EU Policy on Training for CSDP*, 7838/17, 3 April 2017, Council of the European Union, para. 33.

[15] A.N.: Involvement in CSDP training at EU level represents a national contribution to the wider CSDP as part of CFSP as well.

pandemic context) to analyse and endorse the recommendations included in the *General Annual Report of the ESDC Activities* (GAREA), which is drafted for the attention and approval of the Steering Committee. The academic calendar for the next calendar year[16] is discussed based on the feedback received from the Member States on the ESDC priorities on training, and the related budged is planned. The EAB September meeting is also the occasion for the chairpersons of various EAB project-oriented Board configurations[17] to report on the achievements during the previous year (new curricula elaborated, new training created, training requirements resulted as part of various workshops and seminars) and discuss the working programme for the new academic year. The chairpersons receive further endorsement of the continuation of their Board configuration (and respectively of their chairmanship for the duration of the new academic year).

European Security and Defence College (ESDC)

The ESDC's main objectives are to:

- enhance the common security and defence culture within the CSDP,
- promote a better understanding of CSDP as an essential part of the EU's CFSP,
- **support** civilian crisis management, including in the field of conflict resolution, and establishing or preserving the conditions for sustainable development.
- **provide**
  - ❖ CSDP mission and operation personnel with a common understanding of the functioning principles of missions and operations, as well as a sense of common European identity,
  - ❖ **training and education** in response to the needs of CSDP missions and operations,
  - ❖ EU institutions and bodies with knowledgeable personnel able to work efficiently on all CSDP and CFSP matters,
  - ❖ EU countries' administrations and staff with knowledgeable personnel familiar with EU policies, institutions and procedures in the field of CFSP.

The ESDC's main tasks are to **organise and conduct training and education activities** in the area of CSDP. These include basic and advanced level courses promoting understanding of the CSDP and CFSP; courses developing leadership; **courses directly supporting CSDP missions and operations**; modules supporting **civilian and military training and education** in the field of CSDP and CFSP

Other ESDC activities include developing of e-learning systems, **producing of training and educational material**, supporting of exchange programmes between training and educational institutes and managing training in the field of conflict prevention and civilian crisis management.

Source: Council Decision (CFSP) 2016/2382 establishing a European Security and Defence College, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A25010101_1

Box no.1: Tasks and objectives of the ESDC

[16] As the fiscal year in the EU starts in January and ends in December, the ESDC is using the calendar year approach for budgeting of the training activities, and the academic calendar is approved in line with the annual budget. So, the ESDC always refers to both academic year (September-August) and academic calendar/fiscal year (January- December).

[17] The ESDC EAB configurations reunite experts from the Member States and from the EU Institutions and Agencies working specifically on topics such as Security Sector Reform/SRR, the *Erasmus Militaire* initiative, missions and operations related training, cyber security and defence training, the sectorial qualification framework for military officer profession or supporting the initiative on European Doctoral School on CSDP.

The second EAB meeting during the ESDC academic year is planned towards the end of the year, in November or December, being the occasion to start the curricula development process. Based on the outcome of the annual conference on training (organised as a side event the days before the EAB meeting), the ESDC curricula is analysed by the network members, with the aim to identify which course curricula should be updated, changed or which new training activities might be included in the training offers under the ESDC auspices. These discussions pave the way for the largest EAB meeting which usually takes place in February the following year (usually organised over two working days) when the new curricula are drafted and endorsed, being submitted to the ESDC Steering Committee for approval. The EAB meeting which prepares the closing of the academic year is planned in May-June, always in the margins of the last residential module of the ESDC flagship CSDP training, namely CSDP High Level Course (a modular training activity dedicated to senior representatives of the Member States, EU Institutions and Agencies and CSDP missions and operations having a significant role in the CSDP). This specific EAB meeting is held in the Member States hosting the fourth module of the CSDP High Level Course, and is dedicated to the approval of the HLC graduation (this course is the only ESDC training where the EAB plays a significant role, as the Board endorses the list of participants in September and approve the graduation and granting the HLC in May/June, at the end of the CSDP programme spanned for the duration of the entire academic year). The EAB meeting is also the occasion for launching of the prioritization exercise, when the Member States are invited to inform the ESDC Secretariat regarding their training priorities for the following calendar year, so the ESDC should adapt the academic calendar to the network members' priorities.

2. Mapping of the Romanian training environment for security and defence (and mostly CSDP): Romanian training providers and the training provided

Romania deploys people (military, police, diplomats, other categories of civilians) for long time under the mandate or command of international actors with global vocation in peacekeeping, crisis management or stabilisation and reconstructions in post-crisis environment.

Romania is a contributor to CSDP missions even before becoming an EU member, at the time when they were stilled as ESDP missions and operations[18]. But this contribution seems being without a serious impact at EU level at least. If notable participation in NATO led missions could be recorded, as some high ranked/highly visible position were already assigned to Romanian personal mainly as part of the deal between partners, the civilian (police staff included) presence in missions under EU, UN and OSCE aegis or mandate got mostly unobserved. As an example: despite deploying police and gendarmerie staff since 1998, with its highest position in 2011 when it ranked as the first EU contributor of civilian seconded personnel for the civilian CSDP missions, Romania recorded its first head of mission only in 2016 (the first ever Romanian head of CSDP mission has been deployed to EUCAP Somalia between 2016-2019). The second head of missions has been recently appointed in October 2020 (the Romanian retired border police officer nominated as Head of EUBAM RAFFAH, a very small CSDP missions with rather a political prominent role in the region than with a genuine CSDP presence, is about to take his new role in the weeks to come).

What is missing from the overall picture? Are the Romanian civilian experts joining the CSDP missions not enough prepared to take over senior roles in the missions? Would the

[18] At the entry into force of the Lisbon Treaty in 2009, the EU's former European Security and Defence Policy (ESDP) has been renamed as Common Security and Defence Policy (CSDP).

lack of sufficient training for Romanian staff be among the reason for not touching high level/command positions? Is this situation linked to a possible lack of coordination between the various actors involved in promoting the experienced Romanian experts, such as line ministries, national training actors, as well as the diplomats in Brussels involved in lobby and negotiation of senior positions in CSDP missions for Romanian nationals? We are not so sure, could only make some assumptions.

Romania has currently eight full-standing members of the ESDC, the Brussels based network of national training institutes involved in the CFSP/CSDP training (Table no.1), but their assiduous work in the European training arena is hardly known or recognised by the national authorities, ministries of defence, interior and foreign affairs among others. For example, in spite of the wide recognition at EU level (CSDP missions included) of the CSDP related training under the ESDC auspices, the training offered since 2012 by the National College of Home Affairs (Colegiul Național de Afaceri Interne/CNAI), part of the Alexandru Ioan Cuza Police Academy[19]), is not taken into account by the Human Resources Management directorate of the Ministry of Internal Affairs as a training counting as basic training of the ministry's experts wishing to work as seconded experts in civilian CSDP missions. Even if the ministry itself (via CNAI) organises a large number of CSDP training according to ESDC approved curricula and based on the training requirements for CSDP missions identified by the relevant EEAS bodies in Brussels, the respective CSDP training are considered as not useful for deployment. Hence, the graduates from the CNAI courses under the ESDC are not allowed to submit their application into the Goalkeeper system[20] managed by the EEAS unless they register and attend a separate course named EUPOL/EU Police and organised annually by another training institution part of the ministry – but a training which is not yet certified by an international/external body and based on a curriculum which is not necessary in line with the EU (or UN) training standards and requirements. Based on our personal professional experiences in education and training and specifically regarding CSDP training[21] and on curricula development for the security and defence, we consider that the training of the national experts for their secondment (deployment) to missions and operations in post-crisis environment should be done in a coordinated matter and based on certified/approved curricula and training programme, so the Romanian experts will gain the

[19] A.N.: The Romanian Police Academy is a university belonging to Ministry of Internal Affairs which offers law enforcement related graduate and postgraduate education according to the national education requirements, being subordinated from educational and methodological point of view to the Ministry of Education and Research.

[20] A.N.: Goalkeeper is a web-based platform that serves Member States, Headquarters and CSDP civilian missions by supporting training, recruitment, capability development and institutional memory for EU/international crisis management. It is made of four on-line modules: Schoolmaster, Registrar, Head-hunter and Governor, each one with specific objectives to support civilian capabilities' development and deployment.

[21] A.N.: The authors of this research paper advocate for the implementation of ESDC curricula in the Romanian CSDP training system, at the same time with the multiplication of efforts of promoting the best prepared and experienced staff for the highly ranked and visible position at EU level they deserve. They have significant experience and expertise in both law enforcement, crisis management and adult education and training: Dr Simina is a former training manager with the ESDC in Brussels (where he has been in charge with the coordination of the curricula development in the framework of the EAB works) and head of training at a leading Romanian organisation involved in civilian capability building for deployment to crisis management missions; Dr Marinescu works with both University of Pitești and the Police Academy (as course director since 2012 for the CNAI training under the ESDC), after 14 years of professional life in Brussels with NATO or EU; while Prof Silași has a longstanding and recognised academic career, a former diplomat who later directed the School of High Comparative European Studies (SISEC) at the West University of Timișoara – the only postgraduate programme in Romania offering Master degrees in High European Studies. Professor Silași is the first Romanian academic to receive the Jean Monnet Professor title, also the recipient of the first Jean Monnet European Centre of Excellence granted to a Romanian university.

same knowledge, skills and competences as the other mission members, regardless their deployment under EU, UN, OSCE or NATO auspices.

Table no. 1: Romanian members of the ESDC network (2020)

No.	Name of the ESDC member	Year of joining
1	National Defence College (*Colegiul Național de Apărare*), together with "Carol I" National Defence University (*Universitatea Națională de Apărare "Carol I"*), including Crisis Management and Multinational Operations Department (*Departamentul Regional de Management al Crizelor și Operații Multinaționale*)	2008 (2018[22])
2	National College of Home Affairs (*Colegiul Național de Afaceri Interne*), together with Alexandru Ioan Cuza Police Academy (*Academia de Poliție "Alexandru Ioan Cuza"*)	June 2012
3	Romanian Diplomatic Institute (*Institutul Diplomatic Român*)	March 2019
4	National Institute for Research and Development in Informatics – ICI Bucharest (*Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București*)	June 2019
5	West University of Timișoara (*Universitatea de Vest din Timișoara*)	April 2020
6	"Ferdinand I" Military Technical Academy *(Academia Tehnică Militară)*	June 2020
7	University Politehnica of Bucharest (*Universitatea Politehnica București*)	June 2020
8	Constanța Maritime University (*Universitatea Maritimă din Constanța*)	September 2020

Source: European Security and Defence College, https://esdc.europa.eu/who-we-are/#partners

The following line ministries are involved in the security and defence training, with a focus on CSDP training under the ESDC auspices: the Ministry of National Defence (with the National Defence University and the National Defence College), Ministry of Internal Affairs (with the Police Academy and its National College of Home Affairs), and the Ministry of Foreign Affairs (with Romanian Diplomatic Institute). There are also research institutes or universities which have recently joined the always expanding ESDC network: the number of the Romanian members multiplied five times in just few years. If originally only the two national Colleges – Defence and Home Affairs – have been involved in CSDP training, other components of their hosting universities have started connection to the ESDC, being followed by "civilian" university or institutes. The Police Academy at such got involved into the *Erasmus Militaire* initiative and allowed the police cadets to join the CSDP Olympiad of 2016 and 2018, while bringing in Romania the initiative in support of the EU Doctoral School on CSDP, a successful ESDC project. The Defence University followed soon in joining the Doctoral School initiative. Then, several universities from Timișoara, Cluj-Napoca, Iași and Bucharest stepped in and embraced the project (some of them also applying for the ESDC membership,). In few years starting with 2016, the number of ESDC actors in Romania grew

[22] A.N.: Being a component of the "Carol I" National Defence University and de-facto ESDC member, CMMOD has been involved so far in one CSDP training under the ESDC on its own in February 2018, while the National Defence College (also under the Defence University) runs most of the training under the ESDC. Another contribution of the University to the ESDC work is the providing of the hosting and management of ESDC servers used by the eLearning system ILIAS since 2008.

from two to ten[23], even if the training delivered by several new members is not much related to CSDP and to CSDP missions' needs. In some cases, the new members are rather covering security and defence at large, as they address cyber security & defence: ICI Bucharest, Technical Academy, University Politehnica of Bucharest and Maritime University of Constanța.

Ministry of Internal Affairs – the main governmental body seconding personnel to CSDP missions, has four training centres covering security and defence (but wrongly enough, only one training provider is considered as offering the necessary training considered for a future deployment).

CNAI is the main Romanian civilian training actor in the CSDP environment, as some 80% of total CSDP related training organised in or by Romania since 2012 has been delivered by the College part of the Police Academy. CNAI was represented in Brussels until recently by 2 seconded national experts, while the Chair of the ESDC EAB is a former associated lecturer. The College has been the first Romanian entity running a Pre-Deployment Training based on the ESDC curriculum. The first EU training on StratCom in the security and defence context has also been initiated with the support of CNAI (the pilot course was one of the major highlight of the training programme under the Romanian Presidency of the Council of the UE in March 2019, and the second iteration has been held in September 2020). All CSDP training delivered by CNAI is in line with the EEAS requirements and follows the ESDC curriculum/evaluation system. The College supported the joining of other Romanian civilian actors/universities to the ESDC network (such as the West University of Timisoara, Babeș-Bolyai University of Cluj-Napoca or the Romanian Diplomatic Institute), which have worked in partnership with the CNAI before applying for own ESDC membership.

CNAI has many strong points. But also, many weak ones: there is rather complicated to employ experts from the Ministry of Internal Affairs as trainers for the CSDP related courses, because the ministry lacks such expertise, the CSDP/CFSP is seen as a niche topic in a Governmental body which is dedicated by its nature to the home affairs domain and the internal security. And those experts with CSDP missions experience are not always allowed to share their knowledge, as they are usually working in totally different domain upon their return home than in the CSDP missions (their experience is almost never used). When the experts are identified and they could join the CSDP training under the ESDC, they face difficulties in connecting the internal security to external security and the CSDP (as happened during training activities addressing capability building, maritime security or disaster relief). It is again the lack of understanding how to connect the dots, the lack of a wider/strategic perspective and of the sense of the EU integrated approach towards crisis (which could be very well applied at national level).

The Institute for Public Order Studies (ISOP) is the oldest training provider on international missions' related instruction at the ministry of interior level, but still need to adapt to the current training environment in security and defence, the training policies and the field realities (it has no external accreditation/certification for the courses yet, even if the institute runs this type of training since 1997). Two types of courses are available at ISOP, "UN Monitors" and "EU Police", both are generally assessed as having low quality and relevance for the future work in crisis management environment: the course participants, after they leave the premises and confront with the reality in the missions, consider that the courses at ISOP do not bringing sufficient added value for would-to-be-deployed personnel. The training focuses mostly on foreign language learning and specialization (language specific terminology for law enforcement activities, plus preparation of future UN SAAT tests in the

[23] A.N.: If Defence University and Police Academy are counted separately than the Defence College and Home Affairs College.

case of UN missions). As already mentioned, the training at ISOP is recognized at ministry level only (the curriculum or the course as such are not following specific standards linked to the missions' training needs or requirements) and are considered as compulsory for police personnel before applying for deployment. The human resources management department of the ministry takes foreign language skills as being the most important, so the main method of selection personnel for deployment (in fact the only recruiting system in place since the early years of deployments, 1998-1999), is the language testing. This has direct results: the best English and French speakers are allowed to submit their applications for deployment, and not the mostly experienced and skilled experts (with probably previous international experience or exposure), but the EEAS/CPCC does not necessarily select the "English professors" for deployment in high secure risk missions to implement the CSDP mandate. The experienced and skilled police and gendarmes officers should find alternative solutions to use their expertise and knowledge as CSDP mission members, and most of them submit applications as contracted personal (Romania has the main share of all contracted personnel in the civilian CSDP missions overall).

The Mihai Viteazu Application School for Officers of the Romanian Gendarmerie is the main training school of the Romanian Gendarmerie which has been created as a result of the cooperation between Romania and France. The training institution is member of the Expertise Network and Francophone Training for Peacekeeping Missions (ENFTPM) of the International Organizations of Francophonie. It organizes basic training for international missions under UN, EU and NATO, which is compulsory for all gendarmerie staff deployed abroad. On the other hand, this training is not recognised by the Human Resource Management directorate of the ministry as corresponding to the basic training before deployment to CSDP missions. With other words, the gendarme staff could be deployed to any NATO mission (as their deployment is managed directly by the Romanian Gendarmerie in direct link with the relevant NATO bodies, and the selection of staff is processed according to NATO rules), but not to UN or EU missions and operations, where the ministry's body intervene in selection. And this, although the course provided at Mihai Viteazu School used to be valid for the gendarme's deployment to EULEX Kosovo (and before to UNMIK Kosovo) between 2002 and 2011. The School has another international recognised training, respectively the *International Superior Course*, considered since 2015 by the UN as in line with the requirements for deployment to UN missions (conforms to the relevant UN Peacekeeping Pre-Deployment Training Standards). In spite of the fact that the *International Superior Course* runs 14 weeks long annual sessions and during the 13 years of existence has instructed participants from 24 countries before their deployment to UN missions, the course is not accepted as relevant for deployment under the ministry of interior either (the course graduates are not allowed to sit for the UN SAAT tests together with the graduates from the ISOP course for "UN Monitors").

Another training centre of the Romanian Gendarmerie, the Ochiuri Gendarmerie Training Centre provides mostly gendarmerie specific tactical and pre-deployment training for crisis management missions (mostly NATO missions, previously prepared the deployment of Former Police Units to EULEX Kosovo). The training centre has been created based on the French Gendarmerie training system, and the institution is linked to French Gendarmerie Training Centre in St. Astier. The Ochiuri Centre has a wide experience in running international crisis management exercises and has participated participation in EU funded projects such as EU Police Services Training (I and II) and currently participates in EU Police and Civilian Services Training project. The gendarme instructors at Ochiuri have designed specific training in support of Iraqis military. The training centre has the necessary infrastructure to organise a future HEAT training, based on ESDC curriculum, which could be

prepared in partnership with the Mihai Viteazu Gendarmerie Application School for Officers (a defence training entity, such as CMMOD, might as well be invited to join such a project).

Out of the large array of training bodies under its command, the Ministry of National Defence participates in the CSDP related training effort with three centres, two belonging to Carol I National Defence University, the National Defence College (CNAp) and the Crisis Management and Multinational Operations Department (CMMOD), plus the Military Technical Academy.

The Romanian traditional training actor in security and defence, CNAp is the first member which joined the ESDC. The entity could be considered as being among the founders of the ESDC, as the Defence University still hosts the Internet servers on which the Internet Distance Learning system is run since 2008. Although NATO-oriented, CNAp deployed one of the first national experts in the ESDC Secretariat in Brussels (national voluntary contribution), the one who set up the current eLearning platform for the ESDC (hosted on the UNAp servers at https://esdc.adlunap.ro). CNAp top level experts in the security and defence field and its courses are considered of reference and a "must go" for the national elite. Using the example of the Police Academy and CNAI, CNAp has started to expand its CSDP related training since 2016. Currently cooperates closely with CNAI and sometimes run CSDP training together under ESDC, such as pre-deployment training, maritime security or strategic communication.

Former NATO Partnership for Peace training centre, currently one of the main training centres at defence level preparing both military and civilians (police and gendarmerie included) for deployment to UN, NATO and UE missions, CMMOD employs particularly good experts, mostly NATO-minded (most training is NATO approved). Its curricula still need to be improved (more EU approach would be needed, with some attempts to implement the ESDC curricula). Have run so far one CSDP training together with the ESDC but could be a valuable partner for the law enforcement training centres under the Ministry of Internal Affairs, especially if the project of a HEAT course will be put in practice. CMMOD is the facto member of the ESDC network, as it is part of the Romanian National Defence University (and could be counted together with the National Defence College, as representing the same entity of origin, or could be counted separately, depending of the immediate interest of those making the statistics). The Centre's former director works currently as training manager within the ESDC Secretariat in Brussels, being in charge among other projects with the Advanced Modular Training and the sectorial qualification framework for the military officer profession.

A new Romanian training actor in the framework of the ESDC is Ferdinand I Military Technic Academy (ATM), which become ESDC member during 2020, bringing its specific expertise in horizontal issues such as cyber security and defence. One training manager (cyber expert) from ATM is employed in the ESDC Secretariat in the Cyber ETEE platform since November 2018.

The Ministry of Foreign Affairs is not a specific training actor, as its status and purpose does not let much room for training activities. However, the ministry is involved in the training with two actors: the Romanian Diplomatic Institute (IDR) and Post-Conflict Reconstruction Training Centre (CeFoR)

The Diplomatic Institute became ESDC member in April 2019, soon after its first involvement in CSDP training together with CNAI and CNAp. During the Presidency of the Council, IDR acted as the host of the third module or the residential CSDP High Level Course 2018-2019. Its legislation is under development in order to facilitate CSDP related training (the changes have been included in the national strategy/plan for the implementation of the

EU Compact for the Civilian CSDP). IDR aims to become a major actor in missions and operations related training.

CeFoR is a sui-generis training centre, in fact only a small unit of the Ministry of Foreign Affairs which, among other tasks, organises and delivers an annual civilian crisis management training dedicated to stabilisation and reconstruction topic. The annual iteration is organised since 2009 in partnership with the Ministry of National Defence and the United Nations Development Programme-Romania (UNDP). Its main goal is to train international experts (representing countries of interest for the Romanian Foreign Ministry from the point of view of the Official Development Assistance/ODA). ODA money is used to fund such training which involves both Romanian participants but mostly staff from Eastern Europe/Caucasus, Asian or African countries. CeFoR does not offer specific CSDP training as was built for a different purpose. However, based on the earlier plans (largely described in the national strategy on civilian capabilities of 2011) but as well in line with the those plans regarding the implementation of the Civilian CSDP Compact, the Ministry of Foreign Affairs shall organise an agency (at the level of department part of the ministry or an independent agency with national competences) to take over the coordination of the Romanian participation in crisis management missions under EU, UN or OSCE (similar to other agencies/structures existing in countries such as Germany, Finland, Sweden or Denmark). Such an agency shall also coordinate the deployment of people to missions and their related training, plus the secondment, funding, logistic support, equipment, and the staff reintegration to the organisation or institution of origin upon their return from the mission abroad. Probably an agency like this could also have a role in promoting the best candidates for senior management positions in CSDP missions and operations. Until the plans are turned into reality, national coordination and coordinated support and promotion of the Romanians deployed to missions remain at desire level.

Along with the line ministries with competences in supporting the Romanian contribution to the overall CSDP as part of the wider CFSP, there are some institutes and universities which become interested in running various forms of CSDP related training, addressing horizontal topics such as cyber security and defence.

The National Institute for Research and Development in Informatics - ICI Bucharest is a new CSDP training actor, member of the ESDC since 2019, having a specific expertise in cyber security and defence, critical infrastructure protection. Ferdinand I Military Technical Academy, University Politehnica of Bucharest and Constanța Maritime University (the newest addition on the list of Romanian members of the ESDC) are all focused on cyber domain and not having a specific training programme in support of the civilian experts to be deployed to CSDP missions and operations. Their involvement in the training programmes organised under the ESDC is linked to the Cyber education, training, exercise and evaluation (Cyber ETEE) platform launched at the ESDC since 2018. The main task of the ETEE platform within the ESDC is the coordination of cyber security and defence training and education for EU Member States, but this type of training is not directly addressing the needs of the CSDP missions and operations.

The West University of Timișoara, like other possible future ESDC members coming among the universities, are interested in developing education programmes which shall enhance the security culture of a wider audience and address the staff of CSDP missions and operations. The universities already run educational programme in security studies, and the ESDC membership come to complement their education offers and to enlarge their expertise and the addressability to a larger target audience (as more experienced personnel interested in future deployments to crisis management missions may return to universities to complete their studies prior engaging in missions abroad). Soon after hosting a CSDP Orientation Course

organised in Timișoara by CNAI together with IDR in December 2019, the West University of Timișoara applied for the ESDC membership in February 2020 and came with a proposal of a course on diplomatic skills for CSDP missions. This new course aims to explore the goals and methods of diplomacy in CSDP operational context, with a major emphasis on new diplomacy (soft power, transnational networks, digital technologies), including a critical understanding of globalisation processes and the related horizontal issues as cyber defence, cyber diplomacy and hybrid threats.

The Romanian universities part of the ESDC network are also participating in the EU Doctoral School on CSDP initiative launched in June 2017 (Romania, through the Police Academy, has been among the 8 Member States co-founding the initiative supported by the ESDC via a dedicated Board configuration). Based on the ESDC rule (which states that the network members should receive agreement from the national ministry of foreign affairs before joining the ESDC), the new members join the network only after they provide the EAB with their plans to develop training under the ESDC auspices (in order to become full standing members, the newcomers should organise at least a training activity in line with the ESDC standards in the two calendar years following the accession) and subsequently receive approval from the Steering Committee. But the universities expressing their intention to support the principles of the ESDC initiative to develop an EU Doctoral School on CSDP will benefit of the academic independence/autonomy and simply join the specific ESDC Board configuration at their rector's decision (because the academic research is not necessarily considered as a national contribution to the EU wider CSDP as part of CFSP, as is the case for the training targeting the staff of the CSDP missions and operations). Currently there are 8 Romanian universities[24] supporting the doctoral initiative, as shown in Table no.2, not all being members of the ESDC network.

Table no. 2: Romanian universities supporting the EU Doctoral School on CSDP

No	Name of the university and City	Year of joining
1	Alexandru Ioan Cuza Police Academy (Bucharest)	2017
2	Carol I National Defence University (Bucharest)	2018
3	West University of Timișoara (Timișoara)	2018
4	Babeș-Bolyai University of Cluj-Napoca (Cluj-Napoca)	2018
5	Mihai Viteazu National Intelligence Academy (Bucharest)	2019
6	Ferdinand I Military Technical Academy (Bucharest)	2019
7	Gheorghe Asachi Technical University of Iași (Iași)	2019
8	University Politehnica of Bucharest (Bucharest)	2019

Source: European Security and Defence College, https://esdc.europa.eu/doctoral-school/

[24] A.N.: Unfortunately, the situation may change soon, considering the recent decision of the education minister to withdraw the accreditation of the Police Academy's doctoral schools, linked to a series of accusation of corruption, fraud and plagiarism. Without a proper doctoral school, the Police Academy may not be allowed to continue as member of the EU initiative, unless the new management convinces both Ministry of Internal Affairs and the Ministry of Education and Research that a new line of doctoral studies – CSDP as part of wider European Studies/International Relations or Security Studies/Political Sciences/Social Sciences (a new research domain created in 2019) could replace the infamous *Public Order and Security*, something unique in the academic world. More details on the doctoral scandal could be found as part of the journalistic investigation at https://pressone.ro/o-solutie-pentru-fabricile-de-plagiate-spargerea-monopolului-universitatilor-militare

3. Policy measures and strategic overview: the way ahead for an enhanced Romanian presence in the crisis management field

At the time when EU Member States like Germany are launching widely appreciated initiatives like the European Centres of Excellence on Civilian Crisis Management, as part of the national efforts to implement the EU Compact for a Civilian CSDP (November 2018), Romania is still struggling with the adoption of its national Strategy for the implementation of the Compact. Even if the EU recommendation of the implementation plan template has been adopted in the first semester of 2019, when Romania was at the helm of the European Union during its Presidency of the Council of the EU, the draft legislative proposal was posted on the decisional transparency section of the Ministry of Foreign Affairs' website in August 2020 only (MAE, 2020). It seems that the negotiations between the line ministries on the tasks, measures and responsibilities took longer than initially expected. However, when the EU Member States gather in Brussels at the end of November 2020 for the annual reporting on the progresses achieved in the implementation of the Civilian Compact, Romania may not have yet the national strategy in place with own implementation plan to be fulfilled.

Why such a national strategy and related implementation/action plan is relevant for our analysis of the CSDP training mapping at national level? Simply because the training seems not being a significant field where appropriate measures are to be taken, as part of the national capability building effort aimed to increasing of the number of Romanian civilian experts to be deployed in crisis management missions and operations, and the quality of their applications for secondment (when the personnel's expertise and training is very relevant). The crisis management related training is briefly mentioned in the action plan annexed to the draft national strategy, at chapter no.5 "*Improving the training offer for candidates/experts seconded to EU missions*"[25]. In spite of the various training actors existing at national level (our study is covering only the institutional training institutions, letting apart the training entities belonging to the civil society or representing private initiatives), the draft national strategy mentions only the Diplomatic Institute and the National Defence University. IDR is seen as a future major actor in CSDP related training (probably the national hub from where the training coordination will happen), with a focus on the necessary legislative measures aimed to enhance the IDR capabilities of running such crisis management training (which is not yet included in its competences according to current legislation, in spite of the IDR membership of the ESDC since 2019).The National Defence University is perceived as supporting training entity, which may offer IDR the necessary venue and technical support in running future CSDP training. No word about the CNAI, the main training actor in the civilian CSDP field, or at least about CNAp, the main National Defence University entity involved in CSDP training under the ESDC, as detailed above. No reference to the extensive Romanian network of ESDC members and de wide array of training opportunities available both at the training institutions belonging to the line ministries and at other universities and institutes. Not even a reference to ISOP, which is still considered as the main training body of the Ministry of Internal Affairs, despite the irrelevance of the training provided.

What other elements in the draft national strategy have attracted our attention: *the estimated implementation calendar and the performance indicators for the action plan*. Significant legislative measures have been planned to happen by November 2020, which is not the case, because the draft document is not yet approved, therefore not binding and not implemented. The chosen performance indicators for the success of CSDP related training

[25] A.N.: Ministry of Foreign Affairs, draft legislation proposal - *Hotărâre a Guvernului pentru Aprobarea Strategiei Naționale pentru implementarea Pactului Civil în domeniul Politicii de Securitate și Apărare Comună a Uniunii Europene*, p.19, URL: http://www.mae.ro/node/2011

were the number of training module implemented by December 2020, the number of trainee and the number of lectors/instructors employed. Any reference on the training needs assessment, prioritization of training activities, quality assurance, training evaluation methodology, curricula development, development of new courses or at least a national version of the mandatory pre-deployment and HEAT training or at least a national projection on a training needs analysis. The training under the ESDC auspices is not explicitly mentioned, as the ESDC is rather seen as a partner organisation – the Romanian training institutions are not mentioned are being part of the ESDC. Cooperation in the ESDC framework is mentioned at the measure no.3 "Improving the exchange of good practice and lessons learned between line ministries with EU Member States / Agencies of EU Member States and the EEAS" at the chapter no.7 "Deepening international cooperation in the field": *Continuing to strengthen cooperation between Romanian training institutions (IDR, Police Academy and National Defence University) and the European Security and Defence College*[26]. This measure shall be implemented on a permanent basis, but any criteria for evaluation are foreseen.

It seems that the policy makers in charge with planning of the Romanian contribution to the CSDP as part of the wider CFSP are not aware about the realities in the training field. Probably some other domains are not properly covered, hence the lack of coordination among national actors and the weak promotion of skilled personal to the senior leadership of CSDP missions and operations.

Having in mind the peculiar approach of the national authorities as regarding the implementation of the necessary measures for the development of proper civilian capabilities able to be successfully deployed to crisis management operations, we are proposing several measures to be considered.

4. Policy measures suggestion in support of an enhanced Romanian presence in the CSDP field

Romania already has an (outdated) National strategy of civilian capabilities development (2011) but its re-evaluation would be paramount for any steps forward. The new strategic document aiming to the enhancement of CSDP participation, discussed and approved at the highest political-strategic level (Supreme Council of National Defence) shall have clear objectives/targets, measures, related funding, deadlines, an effective action plan and clearly defined responsible authorities (and more coordination). Such a strategic document should link to the national effort for the implementation of the EU Compact for Civilian CSDP (which has a limited time frame, until 2023) and should derive from the National Defence Strategy[27]. It should also refer to a related strategic communications campaign/strategy.

Another strategic document which should be envisaged by the line ministries, for the implementation of the new National strategy of civilian capabilities development, might be a national strategy for CSDP related training, with the aim of establishing coordination and collaboration between training actors, defining of training priorities and identifying of the necessary financial resources.

[26] *Ibidem*, p.21.
[27] A.N.: The National Defence Strategy for 2020-2024 was approved on 30 June 2020 and published on 1 July 2020.

5. Suggested measures at training/operative level for an enhanced Romanian civilian CSDP

Establishing of a consortium between the main CSDP training actors from the line ministers could be the first measure taken in order to enhance the cooperation between National College of Home Affairs (Ministry of Internal Affairs), National Defence College (Ministry of National Defence) and the Romanian Diplomatic Institute (Ministry of Foreign Affairs), all three being the main actors in the CSDP training and also ESDC members. The members of the future "Romanian CSDP Consortium" shall work to build on a common core curriculum for the training dedicated to Romanian staff deployed to crisis management missions and operations and to organise CSDP courses together on a permanent basis (as a way to avoid inappropriate competitions in accessing on the ESDC annual training calendar).

The Consortium would be the right actor charged with the task of periodically running of the training needs analysis at the wide national level, to link training providers and training products to the real needs (based on the strategic view on deployments and the need for trained staff to be deployed).

At the same time, all training organised at national level and addressing the national audience should be provided in English and should be open to international audience (like the CMMOD approach and in line with the ESDC requirements), even if the respective national courses are not included in the ESDC annual calendar and are not financed from ESDC funds. The national courses, alike those run under the ESDC auspices, shall be promoted via the EEAS based Schoolmaster platform[28].

According to the training needs analysis at EEAS/CPCC and EUMS level, and respectively to CEPOL operational training needs analysis[29], pre-deployment and HEAT courses are very important for the successfully deployment of national seconded experts, especially when considering the law enforcement personal which is not generally used and trained to work in high risky and security hostile environments. Establishing of national pre-deployment training activities and HEAT courses should be included on the priority list of the future Romanian CSDP Consortium. The pre-deployment course should follow the ESDC approach and the related curriculum, while the HEAT course may be organised with a civil-military approach in mind, for example as a cooperative initiative of both CMMOD from the Defence University and Mihai Viteazu Application Gendarmerie School, with the support of Ochiuri Gendarmerie Training Centre.

Finally, but not as the last option, strategic communications measures to promote the Romania's efforts and the skilled civilian experts should be planned and implemented along with the other measures taken for an enhanced Romanian CSDP. Building and promoting the correct image of the personnel identified as having potential for promotion to high level positions within the EU structures and in the missions may as well support the backstage negotiations of the relevant authorities aiming to put the suitable Romanian experts on the deserved senior management positions in CSDP missions and operations.

However, all suggested measures or any other plans cannot be successful without a coordinated approach and a real understanding by all actors of the level of ambition defined at

[28] A.N.: In the area of training, the Schoolmaster database https://goalkeeper.eeas.europa.eu is an information hub aimed at capturing and making easily accessible at a single location the largest possible amount of information on training opportunities relevant to CSDP and international crisis management in general for both specialized audiences and the wider interested public.

[29] A.N.: The Operational Training Needs Analysis on CSDP Missions (European Union Agency for Law Enforcement Training -CEPOL, May 2018, found that the most relevant training requirement for law enforcement officials when addressing crisis management are pre-deployment training (93.33% of MSs found it relevant) followed by hostile environment management (86.67%).

national level. And for this, political decision and commitment is of utmost importance. Political decision and appropriate funding may be the key. In order to reach the high level of ambition of a future National strategy of civilian capabilities development, the appropriate funding (financial resources) for training should be identified. At this moment, training is perceived as the last element to be considered before deployment, and funding for training (and especially for the mandatory pre-deployment training) is never identified, nor planned[30].

Without a strong political commitment toward the implementation of the strategic national project, the lack of coordination at national level and the insufficient allocation of financial resources for training may not allow further steps in the development of the desired civilian capabilities able to successfully deploy to crisis management missions.

BIBLIOGRAPHY:

1. CEPOL, *Operational Training Needs Analysis on CSDP Missions*, European Union Agency for Law Enforcement Training, May 2018, URL: https://www. cepol.europa.eu/media/news/cepol-management-board-approves-pilot-otna-reports-csdp-missions-counterterrorism
2. COM, Joint Communication to the European Parliament and the Council, *'The EU's comprehensive approach to external conflict and crises'*, JOIN/2013/030 final, European Commission, URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52013JC0030
3. Council, *Annual 2013 CSDP Lessons Report*, 8015/14, 20 March 2014, Council of the European Union, URL: http://data.consilium.europa.eu/doc/document/ST-6777-2015-INIT/en/pdf
4. Council, *Council Decision (CFSP) 2016/2382 establishing a European Security and Defence College (ESDC) and repealing Decision 2013/189/CFSP*, Council of the European Union, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= LEGISSUM%3A25010101_1
5. Council, *EU Policy on Training for CSDP*, 7838/17, 3 April 2017, Council of the European Union, URL: https://data.consilium.europa.eu/doc/document/ST-8677-2018-INIT/en/pdf
6. Council, *Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on the establishment of a Civilian CSDP Compact*, 14305/18, 19 November 2018, Council of the European Union, URL: https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/civilian-common-security-and-defence-policy-eu-strengthens-its-capacities-to-act/
7. EUNPACK, *Understanding the EU's crisis response toolbox and decision-making processes, Good intentions, mixed results – A conflict sensitive unpacking of the EU comprehensive approach to conflict and crisis mechanisms*, Deliverable 4.1, version 30.09.2016, Norwegian Institute of International Affairs (NUPI), retrieved at 19.10.2020 URL: http://www.eunpack.eu/the-project/work-packages/eu-crisis-response-and-management-wp4
8. EUPARL, *Civilian and military personnel in CSDP missions and operations*, European Parliament, Directorate-General for External Policies, Policy Department, February 2017, EP/EXPO/B/SEDE/2016/02
9. EUPARL, *The Civilian CSDP Compact. A stronger EU footprint in a connected, complex, contested world*, Tania Lațici, European Parliamentary Research Service, Members' Research Service, PE 630.295, March 2019.

[30] A.N.: Romanian authorities currently deploying personnel to CSDP missions are not providing the mandatory pre-deployment training, nor sending their staff to the pre-deployment training sessions organised by the ESDC.

10. MAE, draft legislation proposal – *Hotărâre a Guvernului pentru Aprobarea Strategiei Naționale pentru implementarea Pactului Civil în domeniul Politicii de Securitate și Apărare Comună a Uniunii Europene*, together with the draft national strategy for the implementation of the Civilian CSDP Compact and related the action plan (*"Strategia Națională pentru implementarea Pactului Civil în domeniul Politicii de Securitate și Apărare Comună a Uniunii Europene și Planul de acțiune al Strategiei Naționale pentru implementarea Pactului Civil în domeniul Politicii de Securitate și Apărare Comună a UE"*), Ministry of Foreign Affairs, 29.10.2020 on the ministry's official website for public debate, section dedicated to the decisional transparency: http://www.mae.ro/node/2011

***Disclaimer**: The views expressed in this article represent solely the personal opinions of the authors, not implying the entities they are representing or the institutions and organisations they are professionally active in.*

DEFENSIVE SYSTEMS AND POLITICS. THE VAUBAN SYSTEM AND THE CASE OF THE ALBA-IULIA FORTRESS

Elena-Loredana FLORESCU
International Relations Student, University of Bucharest, Faculty of Political Science
Architecture Student, "Ion Mincu" University of Architecture and Urbanism, Bucharest, Romania. E-mail: elenaloredanaflorescu@gmail.com

Abstract: *The Italian fortress of Palmanova, built in 1593 and designed by Gulio Savorgnan represented a turning point in the studies of the military engineers of that time. The French engineer Sébastien Le Prestre de Vauban, through the fortress of Neuf-Brisach, created the "Vauban defence system", reminiscing of the layout provided by the fortress of Palmanova, approximatively 100 years later. In this paper I intend to analyse the reason why, in 1711, the appointed architect Giovanni Morando Visconti used the Vauban defence system in designing the Alba fortress in the present-day Romania. Following the political and historical background that led to the building of these fortresses and the strategical points that they represent, I intend to identify the similarities between them and whether following an architecture that is based on the ideal city of Renaissance represents a political statement.*

Keywords: *fortress; strategic points; military engineer; defence system; political statement.*

Introduction

Military architecture has seen an increase in its evolution during the fourteenth century after the utilization of the artillery began to be a regular method in a siege warfare. The general defence points of fortresses during the Middle Ages, which served as obstacles during attacks, such as high towers, gatehouses and walls, represented vulnerable targets, due to the distance that guns created between belligerents. A fortified place that would serve as a place from which guns could be fired was required in order to keep up with the progress of the artillery.[1]

The subject of studying military affairs became a field of interest for many scholars and intellectuals, as the money that was drawn from this market represented a point of attraction for them. Therefore, the subject of fortification was put to intensive study and various methods of defence were put up for discussion.

Changes in the general shape of the fortress became to appear, with the emphasis being on gun batteries that were low-lying and firing outwards. Their protection was assured by ditches up to 40 feet deep and thick earth banks. Instead of being vertical, fortifications began to be horizontal, so that cannons could not affect as much the defensive walls. The new walls were with sloping faces, thick and low.[2]

Military architects and engineers developed the fortress into a shape that was more geometrical, angular, solid, characterized by a bastioned outline and a half-sunken profile. After the campaign of King Charles VIII of France, who had a mobile artillery, launched in

[1] Paddy Griffith, "The Vauban Fortifications of France", Osprey Publishing, 2006, p. 39.
[2] Jean-Denis G., G. Lepage, "Vauban and the French Military under Louis XIV/An illustrated History of Fortifications and Strategies", Mc Farland & Company, Inc. Publishers, 2009, pp. 59-60.

Italy in 1494, the medieval fortifications with their high towers and walls were not up to the expectations and their weak points began to appear even more visible.

Medieval castles and their romantic vision were dependent on the equilibrium between the power of the gunpowder, with its new technologies and techniques that developed with its help and the wall's resistance. During the 16th and the 17th century, Europe knew a discrepancy between the frailty of the attacks and the power of the fortresses' defence systems.[3]

Even though the creator of the bastion is not known, the technique of using bastioned fortifications knew a rapid development all over Europe in the first decade of the sixteenth century. Its use meant that a bombardment could pe resisted upon and the enemies could be held at a distance, while the bastion would also serve as a defending fire platform.

The cost of this type of defence system was big: it meant that vertical fortification, which had been built and designed over several centuries and spread throughout the continent needed to be replaced. The price of the new type of construction could only be supported by people in places of power, such as popes, kings and emperors or by independent, rich cities. The bastioned fortification and appearance of gunpowder represented the end of an era, when the state could not hold the monopoly in the matters of national defence.[4]

An example of how successful the bastioned system could be is represented by the fortress of Palmanova, designed by Giulio Savorgnan in 1593, by the order of the Serenissima Repubblica di Venezia. One of the most preserved examples of star-shaped bastioned fortifications, the fortress of Palmanova remained unconquered for more than 200 years, until 1797 when it was defeated by Napoleon. [5]

The Vauban System

During the reign of Louis XIV, Sébastien le Prestre de Vauban was the premier engineer for both urban fortifications and sieges. After Louis XIV's rule reached the peak of its fame, through the Treaty of Nimegue, Vauban's career also developed when he was appointed commissaire-général of fortifications in January 1678. [6] He is approximated to have fortified between 92 and 150 places, either partially or completely.[7]

Vauban's regular designs exemplified the adaptation of pre-existing fortresses to match his ideals. These fortresses were usually places that he would had won after a siege and went back a few decades or sometimes originated in the Middle Ages. Due to the fact that he was the one to conquer them, it was easier for him to design plans that would then be enhanced by French engineers. In his scheme of national defence, he would sometimes expand the fortresses to represent a greater role than before. Therefore, most of its work could be seen as "improvements" or "modernizations". [8]

During the reign of Louis XIV, the bastioned fortifications witnessed the most elaborated constructions and reached the apogee of their fame. Vauban benefited of freedom of action and a large budget that enabled him to apply his principles and vision for the defence

[3] Jamel Ostwald, "Vauban under Siege/ Engineering Efficiency and Martial Vigor in the War of the Spanish Succession", *History of Warfare*, Volume 41, Brill, 2007, p. 1.
[4] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 62.
[5] ***, "Fortress Town of Palmanova", URL: https://whc.unesco.org/en/tentativelists/1154/, accessed on 23.08.2020
[6] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", *op. cit*. p. 18.
[7] *Ibidem*, p. 141.
[8] Paddy Griffith, "The Vauban Fortifications of France", Osprey Publishing, 2006, p. 21.

of France. The realm of Louis XIV represented, for military architects and engineers, a training ground that led to important changes in the urban landscape.

Vauban's work is traditionally known as being divided into three fortification "systems", even though he never thought about them as a "system" at all, as his intention was for his fortresses to pay attention to the local landscape and the problems that they faced in the urban context. His followers, as they practiced his methods, transformed them into what is known today as the Vauban System in order for them to understand his way of working and applying the different design techniques. The classification system was realized during the 18th century.

The first Vauban system is represented by the masonry bastioned front, which is around 330 meters long. Based on a synthesis of the works of De Ville and Blaise de Pagan, his predecessors, the bastioned front incorporates "bastions with or without orillons, a covered way with arms emplacements, advance works and a glacis".[9] With the adequate modulations and adaptations to the local context, this system was applied to most of the fortresses that were designed by Vauban. This system can be observed in the urban defences of the citadels of Lille, Bayonne, Saint-Martin-de-Ré and others.

The disadvantage of the first system was the fact that the defence mechanism was organized around one single focal wall. If, during an attack, a bastion's defenders were put out of action, the adjacent bastions were left without a defence and the collapse of the defence was inevitable due to the disorganization that was produced.

The solution to this problem was sought through the creation of the second system, as the 18th and 19th century theorists claimed. Vauban divided the main wall into two separated and autonomous walls that were separated by a ditch in order to create a front that had a significant depth. The fighting line, called "enceinte de combat", was the first line and encompassed a covered way, counterguards (or detached bastions), demi-lune and tenailles. This external line worked as an envelope, due to the fact that narrow ditches separated the elements and small bridges crossed them, as they created a continuous effect.

The second line was higher than the first one in order to be able to command it and it was called "enceinte de sureté", or the safety line. Due to the towers that were two-story tall and polygonal bastioned, and built in order to contain artillery that could fire through portholes and hide within bombproof casemates, the second line was built with the intention of working as a close-range defence. Even when the first line was conquered and breeched, the safety line was still intact.

The third system represented an enhancement to the second system, with an increase in the defence of the ditch by fitting small flanks in the internal wall enclosure. Moreover, a reduit and a ditch were also added to the demi-lunes. The volume of the masonry of the internal main walls was reduced by making the superior part of it out of thick earth layers, which also increased the resistance of the wall to the enemy fire. The very expensive third system was only applied to Neuf-Brisach.[10]

[9] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 73.
[10] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 76.

Neuf-Brisach fortress

After the Treaty of Nimegue in 1678, the province of Alsace officially became part of the French Empire. Strasbourg, the main city of the province, was finally reunited in 1681.[11] On the southern Rhine, the province of Alsace and the French Empire were linked only by two bridges. One of the bridges led to Brisach and the other one from the city of Strasbourg to the fort of Kehl. [12]

Brisach, a German town, situated on the right bank of the River Rhine, represented a strategic point for the French, as being the only town that had crossing of the river in that part of the territory. During the French occupation of Brisach, from 1648 to 1697, Vauban fortified the town, designing for it twelve bastions, a ditch and seven demi-lunes. [13]

In 1687, the Treaty of Rijswick obliged Louis XIV to give back Brisach, Kehl and Freibug-im-Breisgau, but was allowed to keep Strasbourg. Having to demolish everything they constructed there, when they had to return the Baden area to Austria, the defence of Alsace was left with a hole between Strasbourg and Huningue. In order to reinforce their position, the king ordered Vauban the construction of a new fortress, on the French left Rhine bank. After searching for new possible construction sites, Vauban chose a place that was facing Brisach, near the village of Volgensheim. The new place was named Neuf-Brisach. [14]

Neuf-Brisach represents the most complete work of Vauban, as being a fortress that was designed from scratch. The fortress was then considered an "immobile machine" of war due to the cost of the attacker's resources in a possible siege. The activation of the troops made the fortress a war machine, while their garrisoning made an actual town out of Neuf-Brisach.[15]

The project included the construction of an octagonal fortified town, armed with a double urban wall, as presented before in detailing the Vauban system: the safety wall, together with bastioned towers and curtain walls, followed by the combat wall, equipped with ravelins, detached bastions and large tenailles. Neuf-Brisach also presents the third Vauban system. The urban wall also presented four gates, provided with a series of defences: bridges, drawbridges, casemates and a guardroom.[16]

The organization of the urban space inside the fortress was made possible due to the dividing of the space into a chessboard pattern consisting of 48 square habitation quarters (or *quartiers*). Out of the 48 quarters, 34 were allocated to civilians, allowing the fortress to have a population capacity of approximately 3,500 people.[17]

When designing the fortress, Vauban took into consideration the quality of life of the garrison, knowing that it represented an important factor in maintaining it in the long term. According to their status (single or married with families), the housing was disposed diagonally between the four gates. Within the ramparts, buildings were limited to two stories, so that they could be lower than the city walls. In the case of buildings coming under fire and

[11] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 180.
[12] Christopher Duffy, "The Fortress in the Age of Vauban and Frederick the Great/ 1680-1789", Routledge& Kegan Paul plc, 1985, p. 19.
[13] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 185.
[14] ***, "Neuf-Brisach", URL: http://www.sites-vauban.org/Neuf-Brisach,730, accessed on 24.08.2020.
[15] John D. Lyons, "The Oxford Handbook of the Baroque", Oxford University Press, 2019, p. 225.
[16] "Neuf-Brisach", http://www.sites-vauban.org/Neuf-Brisach,730, accessed on 24.08.2020.
[17] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 186.

collapsing during an attack, streets were designed very wide so that their remains would not block the troops' passing.

Alba Carolina fortress

The building of the Alba Carolina fortress appears in a historical context when Western Europe Monarchs desired to eliminate the Ottoman Empire in Europe and to continue their expansion through Eastern Europe, in order to gain new unknown territories. The control over the Principality of Transylvania becomes the core dispute between the Ottoman and the Hapsburg Empires. Knowing a spectacular bloom, the Habsburg Monarchy is highly placed in the hereditary possessions of the Austrian and stands out as the great European power, able to control Central Europe.

Due to the growing tensions happening in Europe, the political status of Transylvania was fastened in the Habsburg Empire, with the Austrian Court transferring the political power from Transylvania to the Imperial Court. Therefore, the favourable framework was established in order for the construction of defensive systems of fortifications to be done in Transylvania. [18] The city of Alba Iulia offered the Austrian Empire quarters to the imperial army in 1687. The masters of the city decided to build another fortification on the same site as the previous city, to relocate the buildings in the fortress and to resettle the population. The project was given to the Italian architect Giovanni Morando Visconti and was approved by Eugene of Savoy. [19]

Giovanni Morando Visconti was the most important military engineer of the Habsburg Empire at the end of the 17th century and the beginning of the 18th. Originating from Curio, Switzerland, he is mentioned in the army payroll cards of the imperial army in 1685, having participated in all of the expeditions against the Ottoman Empire, including the siege of Belgrade in 1688. In 1691 he was detached in Transylvania to help conduct the constructions of the fortified cities which would become garrisons for the imperial troops in the new conquered territory. [20]

Visconti drew the plans for the new fortification in 1711, and in 1714 the construction began. The old city was demolished, leaving a surface of approximatively 120ha free for the new project. The star-shaped fortification based on a simple programme of the Vauban system has three rows of defensive walls, 7 bastions each carrying a saint's name (excepting the Trinity Bastion, which was the largest), that alternate with the same number of ravelins.

The bastions and ravelins are separated by deep moats and entered by vaulted passages. The material chosen for the bastions was brick masonry that was filled with wattles and mud and had a thickness of 2.5 meters at the base and a height of 12 meters. Two of the bastions, built earlier in the 17th century on the southern side were transformed into artillery platforms, due to the fact that the fortification was intended to use the artillery.[21]

Both Neuf-Brisach and Alba Carolina represented strategic points at the time of their construction. Neuf-Brisach represented a consolidating point for Louis XIV in order to maintain the line of defence in the Alsace region. The place that was chosen for the fortress was in the proximity of the previous fortification that had to be demolished. [22]

---

[18] Danil Sabau, Scientific coordinator Cornel Tatai Balta, Ph.D. Thesis "Morphological Characteristics of Baroque Sculpture in Vauban Bastionary Fortifications of Transylvania", The Ministry of National Education "1 Decembrie 1918", University of Alba Iulia, Faculty of History and Philosophy, 2014, p. 9.

[19] ***, "The fortress- Alba Carolina Vauban-type bastioned fortification", URL: http://memoriaurbis.apulum.ro/en/story/33, accessed on 27.08.2020

[20] Gheorghe Anghel, "290 de ani de la fondarea cetatii bastionare din Alba Iulia'', URL: https://www.dacoromania-alba.ro/nr23/290.htm, accessed on 27.08.2020.

[21] ***, "The fortress- Alba Carolina Vauban-type bastioned fortification", URL: http://memoriaurbis.apulum.ro/en/story/33, accessed on 27.08.2020.

[22] Paddy Griffith, "The Vauban Fortifications of France", Osprey Publishing, 2006, p. 21.

Alba Carolina was integrated as a part in the south-eastern defence system of the Habsburg Empire, among with Timisoara, Belgrade, Arad, Oradea and Ada-Kaled. By choosing the Vauban system that was suitable for a fortress destined to be military and defensive, the arsenal of the province could be deposited in the fortress, along with housing the barracks and the headquarters of military chiefs. The fortification also kept the munitions and the weapons required by the Transylvanian troops and the gold that was produced in the Apuseni Mountains. [23]

The two fortresses also served as propaganda, through their strategic positions and architecture. For the construction of Neuf-Brisach, which also was the first fortress that was made from the ground by Vauban, Louis XIV chose the best and the most expensive out of three designs proposed by the military engineer. Being finished only three years later and with its exorbitant cost, Louis XIV demonstrated the abilities of its military engineers and the fact that the Empire is ready to undergo huge costs for its defence system. [24]

Propaganda in the case of the Alba Carolina is easily witnessed through the monumental Gate of Charles, which represents the third gate. The gate presents sculptures and reliefs on the both western and eastern facades and is the most richly adorned. 30,000 florins were spent at that time for its production by the capital, Vienna. As a monument that is dedicated to Marshal Eugene of Savoy for his success in the expulsion of Ottomans from Central Europe and also for the construction of the fortress, it also reminds the people that pass by about the one ruler of the Hapsburg Empire through the equestrian statue of Emperor Charles VI.[25]

For the next 150 years after the passing of Vauban, French engineers continued to practice his legacy, following his "book of rules" that he laid down. Due to the fact that common sense served as a base for his general approach in designing, many of his fortifications passed the test of time through the wars of the 18th century and the Napoleonic era. The change in the armaments that took place in the 1850s is the fact that caused a radical change in fortress design, putting an end to another trend of fortifications.[26] Neuf-Brisach is a great example of a fortress that until it was besieged in 1870 and taken by the Prussians, it was not troubled by war. [27] Moreover, Alba Carolina successfully faced a four-month long siege in 1849 by the Hungarians. A direct attack was not initiated because the Hungarians decided that the chances for them to win are higher with a siege, waiting for the fortress to run out of resources.[28]

Conclusions

After the fourteenth century, military architecture knew a transformation in its defence mechanisms due to the beginning of the utilization of the artillery. This transformation meant that the costs of the new types of fortifications risen and could be supported by rich cities and people in places of power. Sébastien le Prestre de Vauban, under the rule of Louis XIV, developed a new design for bastioned fortifications that included three lines of defence, known as the Vauban System.

---

[23] "The fortress – Alba Carolina Vauban-type bastioned fortification", URL: http://memoriaurbis.apulum.ro/en/story/33, accessed on 28.08.2020.

[24] Jean-Denis G.G. Lepage, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", Mc Farland & Company, Inc. Publishers, 2009, p. 185.

[25] ***, "The fortress – Alba Carolina Vauban-type bastioned fortification", http://memoriaurbis. apulum.ro/en/story/33, accessed on 28.08.2020.

[26] Paddy Griffith, "The Vauban Fortifications of France", Osprey Publishing, 2006, p. 56.

[27] Jean-Denis G.G.Lepage, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", Mc Farland& Company, Inc. Publishers, 2009, p. 187.

[28] Liviu Zgarciu, "Cetatea Alba-Carolina. Unicul asediu: 25 martie-27 iulie 1849", https://www.historia.ro/sectiune/general/articol/cetatea-alba-carolina-unicul-asediu-25-martie-27-iulie-1849, accessed on 13.10.2020.

As a design that he created from the beginning, Neuf-Brisach, a fortress situated on the French left Rhine bank is considered to be Vauban's most complete work. The new fortress, built after the Treaty of Rijswijk that left the defence of Alsace uneven, had an octagonal shape and presented the three lines of defence of the Vauban system.

Following the successful model of Neuf-Brisach, the architect commissioned to design a fortress for the Habsburg Empire in Transylvania, Giovanni Morando Visconti decided to create a bastioned fortification. The Alba Carolina fortress follows a simple programme of the Vauban system and presents 7 bastions, three defensive walls and ravelins.

Besides the Vauban System, the two mentioned fortress, Neuf-Brisach and Alba Carolina have three more political issues in common: they represented strategic points at the time of their construction, served as propaganda for strengthening the image of their contractors and represented a political statement through their efficiency and resistance over time in the face of the enemies.

Neuf-Brisach could represent the culmination of the bastion fortification, an ideal to which cities could only aspire to reach its image of perfection, one of these being the Alba Carolina fortress. Réne Descartes said in "Discourse on the Method of Rightly Conducting the Reason and Seeking Truth in the Field of Science":

"Those ancient towns which were originally nothing but hamlets, and in the course of time have become great cities, are ordinarily very badly arranged compared to one of the symmetrical metropolitan districts which a city planner has laid out on an open plain according to his own designs. It is true that when we consider their buildings one by one, there is often as much beauty in the first city as in the second, or even more; nevertheless, we observe how they are arranged".[29]

BIBLIOGRAPHY:

1. ***, "Fortress Town of Palmanova", URL: https://whc.unesco.org/ en/tentativelists/1154/
2. ***, "Neuf-Brisach", URL: http://www.sites-vauban.org/Neuf-Brisach
3. ***, "The fortress- Alba Carolina Vauban-type bastioned fortification", URL: http://memoriaurbis.apulum.ro/en/story/33
4. ANGHEL, Gheorghe, "290 de ani de la fondarea cetatii bastionare din Alba Iulia'', URL : https://www.dacoromania-alba.ro/nr23/290.htm
5. DESCARTES, Réne, "Discourse on the Method of Rightly Conducting the Reason and Seeking Truth in the Field of Science".
6. DUFFY, Christopher, "The Fortress in the Age of Vauban and Frederick the Great/ 1680-1789", Routledge& Kegan Paul plc, 1985.
7. G.G.LEPAGE, Jean-Denis, "Vauban and the French Military under Louis XIV/ An illustrated History of Fortifications and Strategies", Mc Farland & Company, Inc. Publishers, 2009.
8. GRIFFITH, Paddy, "The Vauban Fortifications of France", Osprey Publishing, 2006.
9. LYONS, John D., "The Oxford Handbook of the Baroque", Oxford University Press, 2019.
10. OSTWALD, Jamel, "Vauban under Siege/ Engineering Efficiency and Martial Vigor in the War of the Spanish Succession", History of Warfare Volume 41, Brill, 2007.
11. SABAU, Danil (Ph.D. Candidate, Scientific coordinator Cornel Tatai Balta), Ph.D. Thesis: "Morphological Characteristics of Baroque Sculpture in Vauban Bastionary Fortifications of Transylvania", The Ministry of National Education "1 Decembrie 1918" University of Alba Iulia, Faculty of History and Philosophy, 2014.
12. ZGARCIU, Liviu, "Cetatea Alba-Carolina. Unicul asediu: 25 martie-27 iulie 1849", URL: https://www.historia.ro/sectiune/general/articol/cetatea-alba-carolina-unicul-asediu-25-martie-27-iulie-1849

[29] Réne Descartes, "Discourse on the Method of Rightly Conducting the Reason and Seeking Truth in the Field of Science".

DEFINING CENTRES OF GRAVITY WITHIN THE STRATEGIC NUCLEAR BALANCE BETWEEN THE UNITED STATES OF AMERICA AND THE RUSSIAN FEDERATION

Mario MARINOV
Ph.D. Candidate, University of Library Studies and Information Technologies, Sofia, Bulgaria. E-mail: mario.v.marinov@gmail.com

Abstract: *The concept of "Centres of Gravity", and its varied interpretations across history, has been a traditional staple when producing comparisons and analysis on competing military organisations and structures. The following paper aims to extend this specific approach to the less conventional state of affairs existing in the "strategic nuclear balance" between the United States of America and the Russian Federation, through the utilisation of traditional interpretations of the concepts involved, their implementation to the given case studies within the scientific method and the overarching interpretation of two competing organisations within the systemic approach. The paper thus identifies the contemporary centres of gravity within the two structures, the specific dynamic that derives from their present relationship and, consequently, the hallmarks of their nuclear strategy.*

Keywords: *centre of gravity; strategic nuclear balance; Russian Federation; United States of America.*

"History teaches that war begins when governments believe the price of aggression is cheap."
Ronald Reagan – 40th President of the United States (1981-1989)

Introduction

As sophisticated beings inclined towards the scientific thought that has come to define our strives and ambitions, it is also natural to examine and seek out those specific factors in our military conflicts that will provide the necessary sets of ideas and thinking ensuring dominance and leading to victory on the field of battle. From the ideas of the *"Kantai Kessen"*, to the ideas of *"Bewegungskrieg"* and the theories on hybrid warfare, there have always been attempts, some more successful than others, to define and find the best way to achieve victory in a given operational domain, historical period, and against a specific adversary.

Some concepts have evolved and been developed and refined to better suit the ever-changing characteristics of warfare. Few, however, have withstood the test of time, and even fewer have continued to be pivotal points of discussion centuries after their inception. The ideas of 18th and 19th century Prussian major-general Carl von Clausewitz, expressed in his seminal collection "*Vom Kriege"* (*On War*), are one example of such a work. Together with works of the likes of Sun Tzu's *"The Art of War"*, *"On War"* has become one of the "holy scriptures" of military though and strategy to the point of continued discussions on their implementation in the contemporary era from the halls of first-year academic courses in military strategy to the planning rooms of modern military operations.

War, in its essence, has seen unprecedented changes in the two centuries since Clausewitz's work was posthumously compiled. The biggest and perhaps most drastic of

these came with the beginning of the *Atomic Era* on August 6th, 1945 and the atomic bombing of Hiroshima during the Second World War, which in turn redefined any perceptions on the future conduct of war. Since the moment of possession of fission and later fusion weapons on both sides in the subsequent Cold War period between the United States of America and the Union of Soviet Socialist Republics, any prospect of achieving a worthwhile victory in a potential conflict became a questionable prospect. A prospect that slipped ever more into irrelevance with the nuclear arms race that came to define the Cold War period, the tens of thousands of nuclear weapons systems stockpiled by the end of it and the bleak prospects of the future they brought with them, for Man had finally truly *"…become Death, the destroyer of worlds"*, as Robert Oppenheimer stated upon witnessing his work.

It is at this point in the history and development of warfare that scholarly opinion shifts to viewing the principal ideas of Clausewitz for achieving a strategic victory over the enemy as no longer applicable[1] – in the nuclear era, and specifically in the relationship between two nuclear superpowers, the concept of military victory, in itself, becomes questionable, for can there be a true victory in a global nuclear exchange?

Whilst Clausewitz's overarching postulations will most certainly continue to be the subject of wide academic and scholarly debate for decades to come, the following paper will focus only on one intrinsic element first defined in *"On War"*, namely that of *"Centres of Gravity"*, or *CoGs* for the sake of brevity, and one, which this paper accepts as possessing a great measure of continued applicability in the nuclear era and in the examination of the relationships and specific characteristics of its principal actors. The paper has as its main object of study the extant *"strategic nuclear balance"* between the United States of America (United States) and the Russian Federation (Russia), which is *viewed as a dynamic process encompassing two interacting and competing complex military organisations*, with the subject being the application of *CoGs* within this dynamic state. Consequently, the principal research objectives are the definition and application of *CoGs* in examining the specific relationship between the two states, the extrapolation of key trends in the development and objectives of their nuclear forces, and the application of *CoGs* in an overarching framework that encompasses these processes. The main theoretical approaches taken and general methodology utilised will include the application of systems theory, organisations theory and contemporary interpretations of defining *CoGs*, within the overall scientific method.

The principal thesis of the following paper is that the nuclear forces of the United States of America and the Russian Federation stand as two competing recursive systems within the higher international system. Examined as two competing military structures they each possess characteristic and dynamic focal points of strength and purpose in their capabilities, examined as Centres of Gravity. The dynamic in the development and the values of these Centres of Gravity are therefore expressed within the extant state of the "strategic nuclear balance" between the two state actors in the international system, where a corresponding Centre of Gravity, necessary for the preservation of peace between the two subsystems, also develops.

To achieve the objectives of the paper the following tasks must be fulfilled to the greatest extend possible within the size constraints, namely:

- Providing a satisfactory definition of the "strategic nuclear balance" through the utilisation of systems theory, organisations theory, as well as the general preconditions for the existence of security within an organisation or system.
- Providing a general definition of "Centres of Gravity" based upon traditional and new interpretations of the concept deriving from "On War", definitions provided both within

[1] John Shephard, *On War: Is Clausewitz Still Relevant*, U.S. Army War College, Carlisle, 1990, pp. 87-91.

contemporary Western military organisations and current academic debate on the term's interpretation and implementation.

- The application of CoGs within the nuclear forces of the United States and Russia and identifying the implementation of the concept within the current characteristics of the two systems.
- Further extending the idea of CoGs outside of the state level and to the specific relationship within the higher international system that defines the "strategic nuclear balance" between the United States and Russia.

1. Defining the "strategic nuclear balance"

For the purposes of this paper a satisfactory definition must first be provided to the concept of the *"strategic nuclear balance"* and what is meant by it. The traditional postulations of general systems theory are further utilised in conjunction with organisations theory to provide the following conclusions:

- First and foremost, the notion of *"balance"* entails the existence of two or more subordinate interacting units or subsystems within a larger system that by the very definition of a system seeks equilibrium in its operations for its continued existence. The overarching system in question is viewed as the *"international system"*, within which a certain balance is to be sought and potentially achieved. This is also the superior system within which the state actors interact – as recursive systems they are affected by the superior system, but are also key to precipitating change within it. [2]
- Within the broader international system state actors are viewed as its structural elements and are themselves viewed as complex social systems and organisations possessing intrinsic sets of capabilities, objectives, values and leadership, as well as underlying cultural, social and historic peculiarities that form the basis for establishing the conduct and substance of the former.
- The principal objective of any organisation, or in the given case any state actor, is to provide for its continued existence through ensuring and maintaining a nominal level of security.[3]As was previously stated, the last 75 years have elevated the existence and possession of nuclear weapons as a principal instrument for ensuring security and preserving the sovereignty of the state. The international system has also been further elevated and established as the principal domain of interaction between state actors in pursuing their objectives.
- The *"strategic"* nature of the balance necessitates the discussion of strategic level assets, defined per the existing treaty framework as *"strategic offensive arms"* and "strategic defensive arms", the latter encompassing anti-ballistic missile (ABM) defence systems.[4] The general definitions can also be seen to include any other assets that have profound and direct relation to the operations of the aforementioned, with examples that can include a wide variety of current and emerging new classes of weapons and technologies such as non-conventional strategic arms, hypersonic glide vehicles, intercontinental nuclear cruise missiles, and strategic unmanned sea-based nuclear platforms.

The notion of the "*strategic nuclear balance"* thus concerns the balance in the strategic nuclear forces between two or more states within the international system. It is a dynamic state with instantaneous values over a given period of time, in which the states in

[2] Evgeni Manev, *Global, Regional and National Security*, Softtrade, Sofia, 2012, pp. 31-36.
[3] Evgeni Manev, "Defining Security – an Organizational Approach", *Journal of Legal Studies*, Vol. XXIII, Burgas, 2016, pp. 262-274.
[4] *Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms*, Prague, April, 2010, pp. 1-2.

question seek security through the pursuit of certain defined objectives in their capabilities in order to ensure deterrence against one another and therefore continued peace and survival.[5] Within the international system the key subsystems seek the establishment of effective mechanisms of interaction that strive to subdue the risk through the creation of a stable and risk-free environment providing set values for ensuring the existence of a state of *"balance"* – the creation of a multilateral system of treaties and enforcement apparatuses is seen as the most effective and principal point of these efforts. The above assumptions can exist at their nominal state under the condition that they involve rational nuclear armed state actors possessing substantial and developed nuclear triads and view nuclear war against one another within their respective strategic doctrines as precursive to total and mutual annihilation – the concept of *"mutually assured destruction"*, colloquially known as *"MAD"*.

Based on the aforementioned the "strategic nuclear balance" within this paper is viewed as chiefly encompassing the USA and Russia due to several factors:

- In total the USA and Russia possess more than 90% of global nuclear weapons stockpiles.
- Both states have completely developed nuclear triads, possessing a larger arsenal and more technologically advanced nuclear weapons arsenal and delivery systems than other nuclear armed states.
- The two states have a profound history of nuclear strategy development and evolution that is intrinsically linked to one another and goes back seven decades. Consequently, both states have an inherent and deep understanding of the opposite's objectives, fears, strategic culture and modus operandi.
- Both states recognised the need for parity in their capabilities in order to diminish the risks of accidental nuclear war and to provide for the existence of a sufficient nuclear arsenal to ensure "minimum deterrence" against the another, materialising in efforts to achieve this on mutual grounds.
- Consequently, both the USA and Russia engaged to ensure the existence of a balance between their capabilities through the creation of a diplomatic framework of treaties and accommodations that became the chief instrument in precipitating the existence of a balance within the international system in the late-Cold War and immediate post-Cold War period.

Even so the *"strategic nuclear balance"* between the USA and Russia is a dynamic process, subject to change both from within the organisational structure and due to external factors originating from the ever-dynamic nature of contemporary geopolitics. Though a substantial reduction in nuclear arms and establishment of a degree of certain parity in past decades, the contemporary geopolitical environment has given impetus to new processes. These have led to revaluations within the internal architecture of the two organisations and given rise to a change in foci of the current and future development of their respective nuclear forces – themselves giving rise to changes in the instantaneous values within the international system leading it away from the point of balance.

2. Defining Centres of Gravity

The next task is to provide further clarification on the concept of *"centres of gravity"*. This is a complex task as the definition within the original work has been subject to semantic differences in translations to the English language and differing interpretations by academic scholars in the years since, attributing diverging overall meanings to the exact nature of the

[5] Mario Marinov, "Systemic Approach for Analyzing the Contemporary Strategic Nuclear Balance as an Element of the International System", *Journal of Knowledge Society and 21st Century Humanism*, University of Library Studies and Information Technologies, Sofia, 2020.

concept. The paper will thus try to construct a framework around those most relevant in their implementation to the overarching topic of the *"strategic nuclear balance"* and its radically different nature from that of conventional warfare where the concept of *CoGs* is most often applied and defined. The methodology of this process is expressed with first providing the baseline definition from Calusewtiz's *"On War"*, presenting contemporary interpretations of the concept, listing the essential elements and requirements that make up the concept and then proceeding within a chosen method for defining *CoG*s in the next chapter.

The traditional concept of *CoGs* first derives from the notion of the *"schwerpunkt"*, elaborated upon in *Book Six* of *"On War"* of the 1976 Howard and Paret translation as „a center of gravity [sic] is always found where the mass is concentrated most densely. It presents the most effective target for a blow; furthermore, the heaviest blow is that struck by the center of gravity [sic]. The same holds true in war"[6] and further elaborated as to its exact nature in Book Eight as "One must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain centre of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[7]

In accepted modern terminology, the final 2020 iteration of *JP 1-02* „Department of Defense Dictionary of Military and Associated Terms", the definition for *CoGs* derives from traditional interpretations and is provided as "the source of power that provides moral or physical strength, freedom of action, or will to act".[8] Contemporary scholars themselves provide varying interpretations and more in-debt elaborations of the concept, two of which provide the basis for further analysis within this paper. Dr. Milan Vego defines *CoGs* in his book „Joint operational warfare: theory and practice" as „a source of "massed" strength – physical or moral – or a source of leverage, whose serious degradation, dislocation, neutralization, or destruction would have the most decisive impact on the enemy's or one's own ability to accomplish a given military objective; tactical, operational, and strategic (theatre-strategic and national/alliance/coalition) CoGs are differentiated; each CoG is related to the corresponding military objective to be accomplished".[9] Dr. Milan Vego further characterises *CoGs* as possessing both military and non-military characteristics, which in turn can include both tangible and non-tangible factors, such as specific leadership and morale. *CoGs* are also stated to exist only after the objectives they relate to have first been determined, but should not be viewed as equating to them[10]. The interpretations of Dr. Vego are a useful instrument in defining *CoGs*, especially on the national level of the two organisations within the broader "strategic nuclear balance", the United States and Russia, due to the applicability of the requirements to the organisational and systems-based approaches, where the objectives within an organisation, as well as the specific internal organisational characteristics are key in finding its corresponding functional state and operational design[11]. This interpretation is also the more applicable one when seeking certain more tangible and concrete *CoGs*, such as those specific to the force composition and key

[6] Carl von Clausewitz, *On War*, Princeton University Press, New Jersey, 1989, p. 485.
[7] *Ibidem*, p. 595.
[8] *DOD Dictionary of Military and Associated Terms*, Office of the Chairman of the Joint Chiefs of Staff, Washington DC: The Joint Staff, 2020, p. 30.
[9] Milan Vego, *Joint operational warfare: theory and practice*, from Ion Chiocea et al, *Defintions of Center of Gravity – Evolution and Interpretations*, Technologies – Military Applications, Simulation and Resources, "Carol I" National Defence University, Bucharest, 2017, p. 43.
[10] Ion Chiorcea et al, *Defintions of Center of Gravity – Evolution and Interpretations*, Technologies – Military Applications, Simulation and Resources, "Carol I" National Defence University, Bucharest, 2017, pp. 43-44.
[11] Ion Chiorcea et al, *Center of Gravity – Essential Element of Operational Design*, Technologies – Military Applications, Simulation and Resources, "Carol I" National Defence University, Bucharest, 2017, pp. 30-31.

elements of the strategic nuclear armed forces of the states in question, whicha re viewed as sources of "massed strength".

Dr. Antulio Echevarria in *Rethinking Clausewitz's Centre of Gravity* provides a differing interpretations and discounts *CoGs* as a *"source of strength"* concluding that *„CoG is not the strength, not the source of strength and not a weakness. CoG is what holds the enemy's force together. CoG is the "focal point" that holds the system together, but only exists if there is a certain degree of connection"*.[12] Thus within the systems-based approach, *CoGs* are viewed as depending on the degree of connectivity and unity within a system. This approach is useful when examining and defining the possible *CoGs* within the higher level of the *"strategic nuclear balance"* expressed in the international system, where the factors deriving from the *CoGs* on the national level materialise in their interaction and purpose into a specific array of less-tangible interconnecting factors. It is through the degradation of these extant systemic connections on the international level, that the *"strategic nuclear balance"* and its desired state can potentially be upset from the point of balance between its two main constituent subsystems.

Based upon these definitions and the greater works of the authors listed, the following general requirements and terms can be derived within the greater concept of *"Centres of Gravity",* and when searching for CoGs within "strategic nuclear balance": multiple *CoGs* can exist within a given system; the existence of the conventional notion of *CoGs* requires the presence of two or more competing systems; *CoGs* encompass those elements specific to the conflict in question*;* the existence of *CoGs* is precluded by the existence of specific objectives within these systems or system and which are part of the overall state of conflict; *CoGs* can have tangible and non-tangible values; *CoGs* can also be defined in the focal points of what holds a system together and prevent its collapse; competing and contrasting *CoGs* in two organisations can be examined as possessing sets of critical strengths and critical weakness intrinsic to each of them.

3. Centres of gravity within the "strategic nuclear balance" between the United States and Russian Federation

Having provided the general definitions and requirements for both the concepts of the *"strategic nuclear balance"* and *"centres of gravity"* the next step is to demonstrate how these coalesce together and how *CoGs* are specifically applied to the complex overarching system of dynamic processes that makes up the "*strategic nuclear balance"* on both the systemic levels of the United States and Russian Federation, as well as on the higher international level.

When examining the relationship between the two complex organisational systems of the United States and Russia and specifically their nuclear forces, the first principal assumption and requirement for the existence of *CoGs* is viewed as the presence of conflict between two competing military organisations, or in the case of this study the more appropriate term *"competition"* will be applied. The United States and Russia, formerly the Soviet Union, present a complex system of historic security interactions intrinsically tied to the development of their respective nuclear forces as critical elements of their state power, military doctrine and general security perceptions within the Cold War and post-Cold War periods. This in itself manifests in a prolonged state of constant competition revolving around the development of the strategic capabilities of their nuclear forces, which are quantitively and qualitatively still tied to one another due to the historical factors of the Cold War, the

[12] Antulio Echevarria, Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine–Again!, U.S. Army War College, 2002, p. 16.

geopolitical power and security implications consequential to their continued existence, as well as the long-time lack of any other potent competing organisation, at least up until recently.

Out of this competition, certain tangible *CoGs* can be derived revolving around the principal organisational objectives, which are seen as the second primary element in defining *CoGs* after the presence of conflict. The organisational objectives within the *"strategic nuclear balance"* are dynamic and follow as a consequence of a wide variety of factors originating both from within and without of the individual organisations that can be technological, economic, and political in nature, and are specific to a set time frame of examination. Furthermore, the organisational objectives and the *CoGs* they entail build upon these factors and are subject to changing historical interpretations and assumptions centred on the possession and application of strategic nuclear arms over the past seven decades. Within the singular unit of interactions between the United States and Russia, the principal objectives can be stated to have undergone a historical transition from a state, and corresponding objectives, focused on ensuring a first-strike-capability in the early Cold War era to a state focused on ensuring deterrence through a powerful and sufficient second-strike-capability in the late-Cold War era, when both sides had fully developed their nuclear triads and overcome any significant quantitative and qualitative imbalances that could have been perceived by either side as providing an imminent edge in a potential first-strike. This latter state effectively ensures that any nuclear exchange would be final, and therefore, as had been stated previously, is preclusive of a worthwhile strategic victory, at least when considering the present state of technological development. It is the desired and for the time being current state of affair for ensuring the physical existence of both organisations and the desired nominal state of a meaningful *"strategic nuclear balance"* between the two. The continued existence of this state, materialised by the coalescence of objectives behind it, can then be attributed to the presence and development of certain elements within the armed forces of each state that contribute to the fulfilment of this primary organisational objective.

The specific elements can be best observed and defined when examining the fulfilment of the organisational objectives in the methods of interactions between the two organisations within the higher order system of existence of the two, the international system. The amalgamation of these objectives in both organisations and within the international system is expressed in the diplomatic framework of treaties, which express the desire of both states to regulate and adhere to a balanced state within the *"strategic nuclear balance"*. This has been historically recognised and has been achieved through the identification of the key elements of their respective strategic nuclear forces that contribute to the greatest extend to the security equation of the *"strategic nuclear balance"* and that guarantee parity in capabilities. It is through the maintaining of parity and therefore deterrence in these elements that an optimal level of security in the international system can be achieved. These bilateral treaties are, building upon previous less-successful attempts, namely the (Anti-Ballistic Missile Treaty (ABM), 1972; Strategic Arms Reduction Treaty (START), 1994; Strategic Offensive Reductions Treaty (SORT), 2003; "New" Strategic Arms Reduction Treaty (New START), 2011. Within these treaties certain critical and tangible factors can be ascertained as primary to the *"strategic nuclear balance"* and based upon the aforementioned treaties and their specific content can then be summarised as consisting of: land-based inter-continental ballistic missiles (ICBMs), submarine-launched-ballistic-missiles (SLBMs), air dropped strategic nuclear weapons, anti-ballistic missile-defences (ABM), and also extending to regulating ground-based and space-based early warning infrastructure and command and control

infrastructure in a limited capacity.[13,14] In ensuring a state of parity exists, both states identify the above categories as consisting of all those essential critical strengths of their nuclear force capabilities that are crucial to their nuclear power vis-à-vis one another, and can be stated to be their "traditional" CoGs. These can be further listed per the New Start Treaty and its stipulations at signing and since coming into force as consisting of:

1. Existing types of ICBMs: (a) for the United States of America, the Minuteman 11, Minuteman 111, and Peacekeeper; (b) for the Russian Federation, the RS-12M, RS-12M2, RS-18, RS-20, RS-24, RS-26, and RS-28.

2. Existing types of SLBMs: (a) for the Russian Federation, the RSM-50, RSM-52, RSM-54, and RSM-56; (b) for the United States of America, the Trident 11.

3. Existing types of heavy bombers are: (a) for the United States of America, the B-52G, B-52H, B-IB, and B-2A; (b) for the Russian Federation, the Tu-95MS and Tu-160.

4. Existing types of ICBM launchers and SLBM launchers: (a) for the Russian Federation, ICBM launchers RS-12M, RS-12M2, RS-18, RS-20, RS-24, RS-26, and RS-28.; SLBM launchers RSM-50, RSM-52, RSM-54, and RSM-56; (b) for the United States of America, ICBM launchers Minuteman 11, Minuteman 111, and Peacekeeper; the SLBM launchers Trident 11.[15,16,17]

In turn the elimination of any critical weaknesses that may come about due to disparities in capabilities is sought after in the principal objectives of the organisations and is fulfilled through the designation of specific numerical values to each type and class of weapons in order to ensure a corresponding level of security in both organisations exists. Based on the above, the assumption can be made that in ensuring the principal objective of the United States and Russia within the "strategic nuclear balance", the "traditional" and historic CoGs within the "strategic nuclear balance" are all those listed elements and their specific numerical values within the armed force structures of the two organisations that fall within the above-listed categories and have been designated as such under the treaties.

However, as was previously discussed, the "strategic nuclear balance" is a dynamic process and the objectives within it and the organisations encompassing it are all subject to dynamic and inevitable transformations. The structure of the treaty framework between the United States and Russia, and the nature of the *CoGs* within is applicable in a given time frame and subject to specific factors, which are all subject to the intrinsic process of change, endemic to any system or organisation. This change and the formation of potential new *CoGs* can be observed in the past two decades as deriving from the changing geopolitical landscape, as well as significant technological advancements, which render elements of former *CoGs*, potentially obsolete.

The rise of the People's Republic of China, a state with a lesser, but rapidly developing nuclear triad, on the world stage as a potent new military and economic competitor, opposed to the unipolar order established in the post-Cold War period is one such main driving factor in the revaluation of the principal objectives in the traditional narrative of the "strategic nuclear balance", specifically by the United States. In addition, the development and proliferation of nuclear weapons and delivery systems in third states, ostensibly hostile to

[13] *Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms*, Prague, April, 2010, pp. 1-2.
[14] *Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems*, Moscow, 1972, pp. 1-3.
[15] *Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms*, Prague, April, 2010, pp. 7-8.
[16] Bureau of Arms Control, Verification and Compliance, New START Treaty Aggregate Numbers of Strategic Offensive Arms, Department of State, Washington DC, May, 2020.
[17] IISS, *The Military Balance 2018*, London, 2018, pp. 14-18; p. 193.

the United States, or its allies, has further changed the strategic landscape and narrative that produced the shared objectives and foundation of the treaty regime governing the *"strategic nuclear balance"*. Against the backdrop of changing geopolitical realities, and not wishing an economically costly and uncertain full-scale nuclear arms race with a multitude of new competing organisations, technological advancements, especially in the realm of guided missile technology, provided one alternative for singular reaction to this new state of affairs for the United States, as well as Russia. As such, the withdrawal of the United States from the ABM treaty in 2002 was followed by the rapid growth and deployment of sea- and land-based ABM systems in the face of the "Aegis" platform and the SM-3 exo-atmospheric interceptor, as well as to a lesser extent the land-based "THAAD". In turn other states, most notably Russia has sought to encourage its own developments in technologies that directly counter US deployments and the potential threat they may pose to traditional strategic offensive nuclear arms and consequently to the established balance within the treaty framework of SORT and later New Start, these being the development of hypersonic glide vehicles for ICBMs, atmospheric hypersonic missiles, as well as the ambiguous Status-6 "Poseidon" underwater strategic nuclear system. Such systems and their wider deployment consequently shift the balance provided by the traditional *CoGs* due to their vastly superior scope in operational potential, and can be identified to form new *CoGs* around the changing organisational objectives of the actors involved and within the current and future *"strategic nuclear balance"*.

4. Centres of gravity within the international system level of the "strategic nuclear balance"

Having established the "centres of gravity" within the two competing military organisations, as well as the state that their empirical values strive towards, the logical elaboration of the concepts discussed would be to further apply the principles of *CoGs* in examining the next order system that encompasses the state of the "strategic nuclear balance". Within the examination of the "strategic nuclear balance", the international system is viewed as the highest order system, which all other systems inhabit and are subservient to. As such, within it a set of principal objectives also develop, which transcend those of the national level organisations and which form the focal point of what is considered the nominal security conditions and state of the broader international system and consequently the *"strategic nuclear balance"*. [18] These conditions and state can be summarized to be that of parity between those subsystems, whose interactions have the potential to greatly degrade and potentially destroy the system. As such the existence of balance between the nuclear capabilities of the United States and Russia is primary to ensuring the continued existence of the international system and therefore peace and stability on the global stage. To achieve this objective, as was previously discussed, the framework of treaties was developed within the international system. This framework presents the focal point of the system, the connectivity in the vast array of factors within it that allow functionality and unity in the closest achievable nominal state of security for all actors involved. These treaties and the subsequent tangible and non-tangible elements that emerge from their existence, such as mechanisms of verification, lines of diplomatic dialogue and trust in addition to set values in strategic offensive and defensive arms form the concrete *CoG* within the international system within the "strategic nuclear balance". The degradation of this *CoG* thus pushes the system away

[18] Mario Marinov, "Systemic Approach for Analyzing the Contemporary Strategic Nuclear Balance as an Element of the International System", *Journal of Knowledge Society and 21st Century Humanism*, University of Library Studies and Information Technologies, Sofia, 2020.

from its nominal values and desired state, and either towards a catastrophic state, or more preferably toward a state where the *CoG* would have to undergo a necessary transformation in order to maintain the stability of the system and encompass a greater variety of factors. In its catastrophic state, where the principal *CoG* is greatly degraded, the international system could witness the full unravelling of the system of checks and balances that have so far maintained parity and stability, and produce a state of uncontrolled nuclear arms competition and rearmament both between the United States and Russia, as well as other forthcoming nuclear powers. This state is undesirable for the international system, and can be viewed as countering current international norms and expectations of contemporary and future global stability and security. Contrary to it, and recognising the deficiencies of the current system in relation to other nuclear powers and the advancements in strategic offensive and defensive technologies, is the transformation of the *CoGs*, in their traditional sense of a framework of treaties to encompass new factors and produce the same results as those witnessed in previous decades.

Conclusion

The notion of the *"strategic nuclear balance"* is of a dynamic process within the international system between two competing organisations, viewed as constituent recursive systems namely the nuclear superpowers of the United States of America and the Russian Federation. Within this process the concept of identifying centres of gravity has been applied through the utilisation of known assumptions and principals in the study of *CoGs*, and examining the specific state and objectives that each of the organisations and their respective nuclear forces strive towards. The paper has thus identified certain tangible *CoGs* as emerging from the historical mutual recognition for the need for deterrence through a state of parity and expressed in the international system of interactions through the creation and enforcement of a specific treaty framework that is the product of past converging objectives in both organisations. These *CoGs* have been identified as consisting of the strategic offensive and strategic defensive nuclear arms that form the centrepiece of regulation and control within the said treaty framework and specifically identified as sea – and land-based strategic nuclear weapons (SLBMs and ICBMs), air-dropped strategic nuclear weapons, as well as anti-ballistic missile (ABM) systems. The dynamic internal processes within the organisations themselves have more recently also produced changing organisational objectives, based upon the emergence of new geopolitical and technological factors, which have been identified to produce certain new potential *CoGs* that possess the capability to become principal such ones in the dynamic to achieve and form a new point of balance. These consequently form the foundations for a future balance between them and the potential obsolescence of the current *CoGs*. Furthermore, the notion of centres of gravity has been extended to encompass the domain that the two national systems inhabit and interact in, namely the international system of relations, identifying the principal *CoG* within it as deriving from the objective and desired state of peace and stability within it and expressed as the current treaty framework, with the future preservation of this state requiring the adaption and change in order to ensure nominal levels of security on the global stage.

BIBLIOGRAPHY:

1. Bureau of Arms Control, Verification and Compliance, *New START Treaty Aggregate Numbers of Strategic Offensive Arms*, Department of State, Washington DC, May, 2020.
2. CHIORCEA Ion et al, *Center of Gravity – Essential Element of Operational Design*, Technologies – Military Applications, Simulation and Resources, "Carol I" National Defense University, Bucharest, 2017.
3. CHIORCEA Ion et al, *Defintions of Center of Gravity – Evolution and Interpretations*, Technologies – Military Applications, Simulation and Resources, "Carol I" National Defence University, Bucharest, 2017.
4. CLAUSEWITZ Carl von, *On War*, Princeton University Press, New Jersey, 1989.
5. Department of State, Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, Prague, April, 2010.
6. Department of State, *Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems*, Moscow, May, 1972.
7. ECHEVARRIA Antulio, *Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine– Again!*, U.S. Army War College, 2002.
8. IISS, *The Military Balance 2018*, London, 2018.
9. MANEV Evgeni, *Defining Security – an Organizational Approach*, Journal of Legal Studies, Vol. XXIII, Burgas, 2016.
10. MANEV Evgeni, *Global, Regional and National Security*, Softtrade, Sofia, 2012.
11. MARINOV Mario, *Systemic Approach for Analyzing the Contemporary Strategic Nuclear Balance as an Element of the International System*, Journal of Knowledge Society and 21st Century Humanism, University of Library Studies and Information Technologies, Sofia, 2020.
12. Office of The Chairman of The Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington DC: The Joint Staff, 2020.
13. SHEPHARD John, *On War: Is Clausewitz Still Relevant?*, U.S. Army War College, Carlisle, 1990.
14. VEGO Milan, *Joint operational warfare: theory and practice*, from Ion Chiocea et al, *Defintions of Center of Gravity – Evolution and Interpretations*, Technologies – Military Applications, Simulation and Resources, "Carol I" National Defence University, Bucharest, 2017.

WOMEN IN THE MILITARY PROFESSION – A BOOK WITH WHITE PAGES?

Marina STĂNESCU
Ph.D. Student and public officer, Ministry of National Defence, Bucharest, Romania.
E-mail: ssimion@mapn.ro

Abstract*: Security is difficult to achieve and, while navigating the seas churned and high stakes situations, our military has to be more than just a sum of highly trained men and women, they have to be effective leaders with skills that exceed military sphere, able to act in an adequate and proportional manner. This article presents women's participation, work and contribution to the Armed Forces development during the second half of the 20th century in Romania. Women and men in this period did not have the same political rights, did not share the same social roles, and could not access the same professional path. Despite facing challenging circumstances, women have assumed active roles and slowly became an integral part of the Armed Forces, showing extraordinary determination and skills. In this article I will explore the main aspects concerning the social, legal, and political conditions affecting women's life and profession.*

Keywords*: Army; gender based roles; boundaries; stereotypes; military career and leadership.*

Introduction

This article presents the general context in which the empowerment of women as a social phenomenon took place, with a focus on their introduction into the military system and their professional course within the system in the second decade of the 20th century. However, it should be noted that the roles, rights, aspirations and motivations of women, as set out in this article, are briefly exposed, possibly even subjective, in the light of personal experience.

Moreover, as this is an area that – with very few exceptions –, has only recently begun to be explored, studies and collections of documents are still limited both in terms of coverage and theoretical – conceptual approach. The Security Council adopted resolution 1325 on women and peace and security on 31 October 2000. This resolution represented a cornerstone for women as it was reaffirming the important role they have in prevention and resolution of conflicts, peace negotiations, peace-building, peacekeeping, humanitarian response and in post-conflict reconstruction and stresses the importance of their equal participation and full involvement in all efforts for the maintenance and promotion of peace and security[1]. Despite the fact that the resolution was adopted in 2000, NATO and its member states started to implement it only ten years later.

From the beginning, it should be emphasized that the article is not intended to be a complaint of the condition of the woman in relation to that of the man, during the research period, but a statistical and factual presentation of the difficulties encountered in the struggle for a military career. Prejudices, social barriers caused by gender stereotypes, as well as the

[1] URL: https://www.un.org/womenwatch/osagi/wps/

eminently masculine specificity of the field were real "milestones" in obtaining a recognition of the right to have a military career.

The way to get through competition and thrive is achieved by radical inclusion some might say that. But only in recent years we shifted the culture from one of imperative masculine command and control to one of inclusion, in which individuals throughout the ranks are empowered to act.

Although the concept of women as leaders is not a novelty, recent trends have shown women breaking through traditional rules, thus pioneering female leadership roles in the military. Women in leadership positions represents a paradigm shift, as we are witnessing more female military officers leading in male-dominated environments, showing femininity, self-efficacy, emotional intelligence, and teamwork skills.

1. The socio-political context

We begin by highlighting the condition of women in the Romanian society in which, until the end of the 19th century, women could not pursue university studies in the provinces inhabited by Romanians. Until 1920, women in Wallachia and Moldova did not have the right to be lawyers. Until 1932, married women in Romania could not own property or not enter into contracts, could not appear in court nor fulfill the role of guardian for their children ("Law of our civil liberation", 1932). Until 1946, women in Romania were not citizens: they did not have the right to vote in parliamentary elections, they could neither be elected to Parliament nor lead ministries[2].

In the second half of the 19th century and in the first half of the 20th century, women's organizations in the territories inhabited by Romanians advocated for the civil and political emancipation of women demanding access to education and work in various professions in which women were excluded, and the right to vote and to be elected in administrative and legislative forums. Especially in the last two decades of the 19th century, women's movements became more and more intense and visible, due to the actions of some large associations with national and international ties, numerous petitions and memoirs addressed to ministries and Parliament, public conferences, and countless articles in central and local publications.

The European context was similar, yet a number of more advanced states had already taken the first steps towards the emancipation of women. Europe was already experiencing the effects of the second industrial revolution at the beginning of the twentieth century, and the widespread introduction of a new form of energy – electricity. Profound changes in the production environment, the development of the banking and stock exchange system and other domains, all made their mark on everyday life. Newspapers, magazines, books and other publications contributed to the creation of a mass culture, and education was opening up more and more democratically to the general public, including women.

But Eastern Europe was lagging behind in several chapters, including technology, social polarization, education and the lack of reforms[3]. Women still continued to be characters active more in the boudoir sphere, continuing to influence indirectly major decisions that concerned society as a whole.

However, even in Western Europe there were enough social disparities and discontent. But soon after, the harsh reality of modern conflict, devastating in all its aspects, dramatically transformed not only the society but also the destinies and mentality of tens of millions of

[2] Ștefania Mihaiescu, *Din istoria feminismului românesc Antologie de texte (1838-1929)*, Polirom, București, pp. 202, 340-353.
[3] Bogdan Antoiu, Alin Matei, *Politică şi societate în secolul XX,* Ministerul Educației şi cercetării, București, 2007, pp. 01-10.

people. The First World War (WWI), through its temporal (four years) and geographical dimensions (Europe, Africa, the Middle East and the Atlantic Ocean) and through the enormous human and material losses suffered by all participating states and by its military characteristics marked, tragically, the sudden end of a world order and the creation of a new general perspective. As for human losses, they are still shocking to this day, it has been a real catastrophe. More than 9 million people (mostly Europeans) have died and more than 6 million have become disabled.

The war, essentially as an instrument of change, has brought about radical restructuring, caused endemic societal reorganizations and, paradoxically, offered women the opportunity to demonstrate abilities which, until then, were exclusively the prerogative of men.

This is the period during which democratic constitutions were adopted bringing universal voting and the election of the President. The newly-emerging, reconstituted or reunited States – Czechoslovakia and Yugoslavia, Poland, Romania – adopt or refine fundamental democratic laws. The hard experiences of a war have required reforms even amongst democracies. Thus, in Great Britain, universal suffrage was introduced, a new electoral law entered into force in Italy, and in France the electoral regime was modified by introducing proportional representation. Furthermore, the democratization was extended beyond all forms of political and social organization, one example being the Regulation of labor issues. Therefore, after the Clemenceau government passed the 8-hour law in 1919, the Treaty of Versailles devoted a special chapter to the organization of social relations.

The period between the two wars is complex, with multiple facets intrinsically connected, and the depth of the changes in the economy, society, morals, ideas and mentalities was not fully understood by contemporary people. For the War-defeated States, the destruction caused, misery of defeat, foreign occupation, weight of the repairs imposed by the peace treaties, political instability caused by the collapse of the respective political regimes, economic disruption and, last but not least, territorial amputations suffered, represented deep traumas and moral wounds that are still endured today, as well as strong reasons for discontent and a desire for rebound. In these areas, democratic intentions have been doomed to failure and revengeful feelings, intolerance, extremist nationalism have increased during the entire interwar period, taking the form of totalitarian, dictatorial and authoritarian political regimes and culminating with another devastating conflagration – the Second World War (WWII).

After WWII, the physical damage was immense and the human loss invaluable. In Europe, the death toll has reached 40 million, and the number of refugees to 30 million. Beyond the loss of human life, it is difficult to calculate the war impact in terms of the birth deficit or of mortality and population aging. The same goes for economic losses: the destruction of material possessions was accompanied by a terrible moral depletion of investment.

2. The woman's condition in the society and her access into the military

Women, throughout this period between the two World Wars were subject to waves of change of extraordinary complexity, going from the status of devoted wives and mothers to that of factory workers, widows or single parents, victims of abuse, unable to defend themselves and without the possibility to legally express their opinions. However, all these unfavorable situations caused them to break down barriers and make their voices heard. Although they have been demanding the right to education and direct political representation since the 19th century, it is only after the end of the First World War that they are beginning to be taken seriously.

We must understand that in that time these requirements, which are absolutely normal today, were seen as something eccentric, a revolutionary movement which, although initially regarded only as an opposition to meeting the society expectations, were essentially a struggle for a normal life.

Feminism was emerging as a movement that claims to fight gender inequality, with the primary aim of asserting women in society by achieving equal rights and freedoms with men. Simone de Beauvoir is the author of the book The Second Sex (Le Deuxième sexe, 1949), the work that can be considered the first attempt at an exhaustive theoretical structuring of the feminist theme. The author captures the feminine posture and patriarchal structures of the time. The typologies identified reflect the perception of the society built through the prism of the tutelary model, the woman being a person without individuality in the public space and especially without associative professional status. It is, even today, one of the most rigid stereotypes of some societies[4].

The initiation of the emancipation movement of women in Romania was considered by the Pașoptist Revolution that had proclaimed "the same teaching for both sexes", although Romanian society as a whole was not prepared to receive such a change. At the end of the 19th century, the "Women's Reunion in Iasi" (which in 1894 was called the "Women's League"), through its vice president, Cornelia Emilian, founded in 1890 the first vocational school in the country with 52 students, graduates obtaining master's degree in lingerie and women's tailoring.

Of course, Romanian feminism can assume a series of important female personalities from the more distant Romanian past, noble figures, such as Mrs. Chiajna, Mrs. Clara, Lady Maria Voichiţa, Mrs. Stanca, Ruxandra Lăpuşneanu, Elisabeta Movilă, Păuna Cantacuzino and others. Often presented negatively because they exceeded their imposed responsibilities, they gained recognition and even political influence.

Later we have Ana Ipătescu, Maria Rosetti, Maria Flechtenmacher, Sofia n. Cocea, Constanța Dunca-Schiau, Dora d'Istria, Calypso Botez, Sofia Nădejde, Smara-Smaranda Gheorghiu, Adela Xenopol, Eugenia de Reuss Ianculescu, Alexandrina Cantacuzino, Maria Băiulescu and many other strong women who broke the barriers of their time. To a large extent, they are unknown to the public, too little being written about them and the diligences made for the emancipation of women. A prominent figure of the period is Queen Maria, who actively supported the granting of universal suffrage to both men and women through the 1923 Constitution, a requirement rejected and considered far too advanced for the Romanian society at that time.

Most of the 20th century is marked by the efforts made by a number of female personalities to be able to have a bank account on their personal name, to be able to be members of the boards of directors of companies, industrial consortia, or to embrace any profession they wished.

WWI forced women to take over men's jobs, and the interwar years were a favorable period for feminist movements in Romania. The redoubt that had to be won, however, remained the right to vote. Just shortly before WWI, a "Women's Rights" society was established, which campaigned for specific feminist purposes: the moral, social, economic and legal emancipation of women. In achieving the proposed goal, the society aimed at a real emancipation, extended to the level of equality of women with men in the political field, which also meant the granting of the right to vote. A freedom that could be difficult to obtain, but used too little. A turning point is the inclusion of women in the paid work area. In 1929, women were given a partial right to vote, in the sense that they could elect and be elected to

[4] URL: http://hist259.web.unc.edu/secondsex/and“Simone de Beauvoir.”, *Wikipedia*, at: https://en.wikipedia.org/wiki/Simone_de_Beauvoir

municipal councils, provided they had completed high school or vocational education, were war widows, or decorated for exceptional service. It was not until 1946 that women in Romania gained this right.

The war and its implications were driving major changes in state policy, as well as the irremediable deterioration of the traditional value system. The Romanian woman proveed her ability to cope with the difficult situation and whether she lived in rural or urban areas, she assumed roles left vacant along with the enrolling of her husband, brother, son or father in the army, going as far as activing participation in armed conflicts. An eloquent example is 2nd Lt. Ecaterina Teodoroiu, a monument of heroism and courage.

But the political sphere, although changed in mentality after WWI, remained reluctant to the opportunity of a debate on the right of women to "citizenship". Despite the dismantling of prejudices or rigid mentalities and attitudes by characters such as Ella Negruzzi, Elena Stoenescu-Caragiani, Smaranda Brăescu or Olga Prezan, the holders of the traditional-innovative state order displayed a reserved attitude. The political approach to the role and position of women remains incohesive in the inter-wars period, lacking in unity and coherence.

The right of women to enter into the Romanian Parliament, won in 1939, was deprived of concreteness with the deterioration of the domestic and international political situation, ending with the outbrake of WWII. The establishment of the communist regime sharply imposed the woman as an "equal socialist worker" with the man. But at the level of the society the issue was far from being assumed and accepted, despite the unequivocal decision of the state authority.

Regardless of the oppression promoted by the communist regime the emancipation of women was experiencing new horizons during this period.

In a specific male area, such as military, women who have chosen this career and excelled in various fields, taking up even leadership positions, have had a strong social impact over time. They have broken the mindset barriers and continue to do so today. There is still not enough said about these women, living models of devotion to the country. They have marked history and continue to do so.

The Romanian Armed Forces, like other modern military of the world, have women holding general ranks and also women fighters, who amaze us with their professionalism shown while fulfilling their missions. Their presence in the Armed Forces, although initially decided as a result of a political conjuncture, later becomes a battle won in court.

Until 1948, American women could only serve in the military during war and only as part of support groups deployed during this period. On 12 June 1948, the Congress approved the Law on women's integration into the Armed Forces, which allowed them to join the military even in peacetime.

The issue of equal opportunities between men and women is still relevant, both internationally within the structures of the UN, EU, NATO, OSCE, and at the national level.

This development is primarily due to women's access to military academies and other military educational institutions, thus obtaining higher education in the field. After 1968, a pre-military youth training program for country defence (PTAP) was organized, with the participation of high school and professional school students, as well as a reduce military training (MTR) for university students, regardless of gender. The students carried out a special program during the schooling period, and they received a military booklet and the rank of reserve officer at the end.

In 1975, Romania had its first promotion of female officers who were mostly assigned to different positions in Military Departments belonging to university centers throughout the country. Women commissioned and non-commissioned officers were initially trained,

separately from men. Nevertheless, these deficiencies were addressed in the 80's and presented in a propaganda campaign of the communist system.

In the early 2000, about 280.000 women were working within NATO member states Armed Forces. Romania, as a NATO Member and the EU Member, has joined the policy of these organizations regarding women's access to the military.

The situation of women and their access to various roles in the military varies considerably from one country to the other. The period between the admission of the first women to the armed forces and the uncensored access to all positions might be very short, or could take several decades, and in some sectors they still do not have access to all positions.

These countries that were the first to open the doors of the military to women are not necessarily the first to give them access to all positions. It is to be noted that during World War I, the Russian Armed Forces already had women soldiers and women pilots, but women did not have access to all positions and equal opportunities for advancement in rank.

At the same time, among NATO member states, two of the six countries where there are still restrictions on women's access to certain military positions began accepting women into their armed forces in 1944 (the Netherlands) and 1946 (Greece). In contrast, in 13 countries that joined NATO after 1999, women already, in theory, have access to all positions.

In Germany, women have had access to civilian positions in the military and access to military positions, especially medical ones since 1975. But it was not until a decision of the Court of Justice of the European Union was delivered, in 2000, which required that all existing posts and hierarchical positions must be made accessible to women. Therefore, women now account for 11.3% (according to the 2018 NATO Summary of the National Reports) of the total staff of the Armed Forces of the member states.

Military career is becoming attractive to women for two main reasons that differ depending on the young aspirant's background, thus the military becomes either social salvation in terms of benefits and stability or a vocation for those who dreamed of pioneering in the field and had high aspirations. Even so, there have been countless voices calling for women to be excluded from the armed forces on the basis of the tradition of associating women with peace and men with war, and of course the physical inability of women to cope with stressful, risky or even life or death decisions.

Women who join the armed forces face an environment designed by and for men. Therefore, recruiting and retaining more women among their staff has become an important issue for the armed forces. However, although Europe's forces have gradually become receptive to the recruitment of women in recent decades, women are still very much in the minority in military roles, especially among the upper ranks.

Women in the military system must cope with many forms of discrimination from the outset and still face rigid guidelines and mentalities that are still ingrained with a purely masculine approach.

The Romanian armed forces have undergone a profound restructuring and transformation process, starting from the structures of the classical socialist army and trying to build a modern and flexible force, compatible with the armies of NATO member countries. If before 1990 Romania had 300,000 troops, then the army was restructured, reaching a number of about 100,000 in 2001 (in 2001, after the army was restructured, it reached a number of about 100,000)[5].

The Armed Forces are a state institution that can use, in an organized and legal way, violence to carry out tasks entrusted to it. As a specialized body for warfare, the armed forces

[5] Institutul pentru studii politice de apărare și istorie militară, coord Petre Otu, *Reforma militară și societatea în România (1878-2008)*, Editura Militară).București, 2009, 321-336.

consist of various specialized structures. The military environment was, by total attribution of masculine characteristics, traditionally recognized and accepted as eminently masculine. The legitimacy of committing acts of violence was socially attributed to the man. Thus, the subunits and combat units, regardless of the category of forces and the type of weapons, were made up of men. This fact was undoubtedly assumed and recognized at the level of the society.

A particularly important aspect, which must be emphasized is that the military was and remains an institution with its own system of organization, leadership and hierarchy, whose activity is carried out in accordance with a series of special legal provisions, in addition to military regulations, orders and dispositions of commanders and chiefs. Thus, the organization, character and evolution of the army are determined by a complex of factors that influence its historical course. As might be expected, the political regime is the most important factor, nonetheless the advances of science and technology also contribute fundamentally to the evolution of the military system. The level of economic development of the country, the social and demographic situation of each state are also factors to be taken into account. There are also a number of other external factors that can have a considerable impact. These include the country's membership in a politico-military alliance and geographical position, which presents many key aspects.

Because of the atypical specificity compared to other state institutions, being a force structure, closed, non-transparent and perhaps even totalitarian in the eyes of some, the introduction of women was difficult and is still a slow process. Their assimilation into military structures was not a linear and continuous process. If in 1975 Romania had the first promotion of women officers, after 1990, women have had access to higher education institutions only in certain specializations on a limited number of places. In post-December 1989 Romania, the idea of professionalizing the armed forces is commencing to become a reality. Until that time, conscription was the central element of the formation of the national force, since the first military units (documentary evidence from the time of ruler Alexandru Ioan Cuza) were established. Since 1990, the first signs of the tendency to accentuate the professionalization of the army appear, both by raising the level of professional qualification of military personnel, and by establishing a new category of military personnel, namely the military hired on a contract basis. It is the moment when the need for qualified forces becomes acute.

All over the world, the women's empowerment movement has also covered the aeronautics sector, with women struggling with prejudices and rigidity of the authorities of the time. Some of the women succeeded with great efforts, expenses and particular political support, to be heard and recognized as true pioneers in the field.

From Romania, the first pilot woman was Elena Caragiani-Stoenescu from Tecuci, who was granted the pilot patent in Paris in 1914. In Europe, the first female pilot is Baroness Raymonde of Roche (France), who was granted the patent in 1910; in America, Harriet Quimby became a pilot in 1911.[6] But their achievements were punctual and disputed by the public and even by the authorities. Many women who were distinguished by the exceptional skills they performed in male fields have remained only "stars", media topics, in competition with men throughout their lives.

The most noticeable, discussed and controversial female personality in the aeronautical field of the period was Amelia Earhart, who made the first transatlantic solo flight on May 20-21, 1932[7]. Although her performance has remained in history, few know her name and accomplishment.

[6] URL: https://en.wikipedia.org/wiki/Timeline_of_women_in_aviation
[7] URL: https://www.britannica.com/biography/Amelia-Earhart

Another example is Smaranda Brăescu, who was the first female parachutist with a patent in Romania, European champion in parachuting (1931) and world champion (in 1932, with a record of 7200 m in Sacramento, USA)[8]. This daring airwoman participated in numerous international aeronautical rallies and, very importantly, participated as a volunteer in World War II, both on the eastern and western fronts.

Florica Ionita represents another extraordinary woman and an eloquent example of tenacity, hard work and total dedication. Her story reveals a personality as modest as it is remarkable, through the perseverance with which she pursued the realization of her dream of a lifetime. Florica graduated from the aviation school attended between January and June 1948, but was denied flight for medical reasons. Nevertheless, she was not discouraged and continued to seek solutions and opportunities to fulfill her dream of flying motorized airplanes.

In 1950 she graduated from the School of Sport Parachuting as head of promotion, demonstrating outstanding abilities and a tenacious personality, mastering both technical and theoretical procedures[9]. During this period, she meets Grigore Baștan, a prominent figure in Romanian skydiving. He is the first paratrooper that achieved the rank of general in the Romanian Army, remaining in history also due to the national record in the parachute jump, recorded in 1970, when he performed a jump from a height of 10,000 m, with a free fall of 7000 m.

Florica Ioniță obtained the parachuting instructor license, as well as the glider pilot license in 1952, when she also became a flight instructor. But then again, her dream was not yet achieved. Through perseverance and hard work, she managed to be admitted to the motor flight school in 1951, and a year later she was also admitted to the flight instructor school, thus fulfilling her aspirations and performing flights daily until the end of her career. But even after the end of this period, she remains dedicated to aviation, being the first woman to be hired as head of air traffic at a civilian airport.

Women like them have remained anonymous in the history of their contemporary society who did not recognized their merits, being deprived of the attention, respect and admiration enjoyed by their male colleagues. Nonetheless, the importance and impact of their actions are overwhelming in raising the status of women in the military system. With the demonstration of exceptional abilities and strength of character by a number of outstanding women, the path to a military career begins to open on several levels. Steps were made in recognizing their right to be part of the military system and the merits of their contribution to the development and modernization of the Army.

Conclusions

After analyzing the information available on this matter and after reading the stories of some of the remarkable women that fought for equal rights, I came to the conclusion that there are two major factors that led to the acceptance and expansion of the role of women in the armed forces.

The first derives from the staff deficiencies and shortcomings experienced by the Armed Forces in times of war and shortly after. The two World Wars have decimated the strength of the armed forces, making it difficult for the military to recruit and maintain a sufficient number of qualified and physically fit men to perform effectively. At the same time, women are increasingly educated, prepared and eager to join the military. Thus, women were

[8] URL: https://radioromaniacultural.ro/documentar-smaranda-braescu-prima-para%E1%B9%A3utista-din-romania/

[9] URL: https://www.agerpres.ro/social/2020/07/15/florica-ionita-prima-femeie-parasutist-de-dupa-cel-de-al-doilea-razboi-mondial-sarbatorita-la-90-de-ani--540943

recruited in increasing numbers and employed in a wider range of military professions, the purpose being to address the shortcomings in the recruitment of qualified men.

Secondly, the equal rights movement for women has led to the claim of equal opportunities in all areas, including national defense, and the gradual abolition of restrictions against them was embraced by the military system.

The emancipation movement takes place amidst increasing access to education and demonstration of unanticipated abilities to manage difficult and dangerous situations. During the two world conflagrations, women not only proved that they have the ability to perform in exclusively male professions but also that they can simultaneously fulfill all the responsibilities deriving from being mothers and spouses.

Armed confrontation experiences of the late twentieth and early twenty-first centuries have highlighted a number of issues regarding women's access to the military and their leadership and execution capabilities. The inclusion of women in military actions, missions and operations in conflict zones around the world has had a considerable impact. As a result of women participating in high-risk missions and operations such as Afghanistan, Iraq, Haiti, Libya, Syria, Saudi Arabia, the Persian Gulf, etc. a series of unprecedented elements that sparked heated discussions and even legislation changes came into sight for the first time. The society was faced with a new reality – women can and want to be part of the active armed forces including in theaters of operations, assuming related risks.

Reports on the Desert Storm operation exposed that women can satisfactorily perform the tasks traditionally performed by men and that they are able to cope with risky combative situations. But like their men's comrades, some women have paid the ultimate price - their own life, not only in armed clashes but also in attacks or accidents. Besides, there have been women that were taken prisoners of war. In addition, reports and statistics published by the US State Department, as well as other relevant civil institutions in other countries, have shown that the emotional impact of a mother's death on an external mission is considerably higher than a father's.

At the same time, there is also a series of controversies and discussions on health and hygiene issues, sexual abuse and harassment, sometimes inflicted by their own colleagues, maternity, physical condition and mental stamina. These controversies continue to be highly debated subjects and sometimes even obstacles to the professional development of women. Some, more or less, are real physical barriers to the advancement of women both in society and in the Armed Forces.

While controversy over the emotional impact of women's victims on the civilian population will continue to exist, as will those mainly driven by gender stereotypes, the percentage of women among the armed forces continues to rise.

As it appears today, the wars of the future certainly require new skills adapted to technological developments. Security threats and risks are constantly evolving. In this context of fragile and volatile security, education and training become essential in the operation of modern and complex weapons systems, regardless of the gender of the members of the armed forces. Over the last decades, not always physical strength has been decisive, but also analysis strategy and flexibility in approaching the problem and if you do not have diversity among Armed Forces, you cannot achieve performance and victory.

BIBLIOGRAPHY:

1. ***, *Reforma militară și societatea în România*, Institutul pentru studii politice de apărare și istorie militară (1878-2008), 2009, Editura Militară, Bucharest.
2. DANDEKER, C, *Femmes combattantes: problemes et perspectives de l'integration des femmes dans l'armee britanique*, Editions Technip & Ophrys, 2003, URL: https://www.cairn.info/revue-francaise-de-sociologie-1-2003-4-page-735.htm
3. HENTEA, C., SCAFEȘ, C., ȘERBĂNESCU, H., *Armata română în misiuni internaționale* (1991-2003), Bucharest, C.N.I. Coresi, 2004.
4. BARBU, D., *Bizanț contra Bizanț. Explorări în cultura politică românească*, 2001, Bucharest, Nemira.
5. CARREIRAS, H., *Gender and the Military. Women in the Armed Forces of Western Democracies*, London and New York, Routledge, 2006.
6. GOODMAN, R. T. (2017*). Gender for the warfare state*. London and New York: Routledge
7. Berindei, D. (2003). *Modernitate și trezire națională. Cultură națională română modernă*. Studii și Eseuri. București: Fundația Pro
8. SAIZU, I. (2003). *Modernizarea României contemporane* (perioada interbelică). Pas și impas. Iași: Alfa
9. PATAPIEVICI, H.R. (2004). *Discernământul modernizării. 7 conferințe despre situația de fapt*. București: Humanitas
10. RADU, S. (2007). *Modernizarea sistemului electoral din România*, Iași: Institutul European
11. SCHIFIRNEȚ, C. (2007). *Formele fără fond. Un brand românesc.* București: Comunicare.ro
12. MIHĂIESCU, Ş. (2002). *Din istoria feminismului românesc: antologie de texte: 1838-1929.* Iaşi: Polirom.
13. STOLTENBERG, J., *Speech by NATO Secretary General Jens Stoltenberg - Ambassador Donald and Vera Blinken Lecture on Global Governance*, Columbia University https://www.nato.int/cps/en/natohq/opinions_169183.htm. 18.08.2020
14. WALKER, K., *A model for femininity and military leadership.* https://doi.org/ 10.1002/jpoc.20086. 18.08.2020
15. Organizational Survey, Annual Reports of the Committee of Women in the NATO Forces. https://www.nato.int/ims/2002/cwinf2002/cwinf-02b.pdf 29.07.2020
16. 2017 NATO Summary of the National Reports. NATO Review 2017 disponibil la: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_09/20190909_190909-2017-Summary-NR-to-NCGP.pdf, 04.08.2020
17. URL: http://hist259.web.unc.edu/secondsex/, 05.09.2020
18. URL: https://www.britannica.com/biography/Amelia-Earhart, 29.10.2020
19. URL: https://en.wikipedia.org/wiki/Simone_de_Beauvoir, 29.10.2020
20. URL: https://en.wikipedia.org/wiki/Timeline_of_women_in_aviation, 29.10.2020
21. URL: https://radioromaniacultural.ro/documentar-smaranda-braescu-prima-para%E1%B9%A3utista-din-romania

CAPITALISM: WHERE TO?

Ionel STOICA
Ministry of National Defence, Bucharest, Romania.
E-mail: jstoica2001@yahoo.com

Abstract*: Mankind is at present at a crossroad, and this fact is valid from a political, economic and social viewpoint. Strong and opposed political and social forces, by the goals they seek, are engaged into a though competition, whose result will decide the way of life for several future generations. From the political point of view, the battle takes place between democracies, on the one hand, and the autocratic regimes, on the other hand. As for the economic and social aspects, the battle develops between the super-rich or the dominant class, and those who struggle to survive. Another facet of this last aspect is represented by the competition that is being carried out between the free market capitalism, combined with the liberal democracy, and the state capitalism, often associated with the illiberal or autocratic political regimes. This paper intends to present and explain the factors that underpin the success of the state capitalism, the way that free market capitalism and the state capitalism coexist at present, as well as the potential for conflict that can appear between the two models of capitalism, with its consequences for global stability. Understanding these aspects is important because the two models of capitalism support distinct models of development and security. We will be focusing more on the state capitalism because we consider that this represents an important force that will shape the global economy in a significant way during the following decades.*

Keywords: *capitalism; free market; autocratic regim; global economy.*

1. Characteristics of the free market capitalism and state capitalism

Free market capitalism is based on the existence of private property of the production means, liberal democracy, free and open competition between the economic agents playing on the market, a reduced and (more or less) discrete presence of the state in the economic activities, with the goal of making financial profit. There are several models of market economies: that Anglo-Saxon[1] (USA, The United Kingdom), that west-European[2] (France, Italy, Spain), the social market economy[3] (Germany, Austria), the market economy specific to the Northern countries[4] (Sweden, Norway, Denmark), the paternalist market economy[5] (Japan) – each of these with its own characteristics (in each of these types of economies the capital plays a certain role, that reflects the ratios between state and market).

[1] A.N.: This economic model supposes that the state exercises a minimal presence in the economy; the private sector is dominant and the large companies have a dominant position in the strategic fields.
[2] A.N.: The state participates, along with the private sector, at the economic activities, and it intervenes into the economic life by specific policies.
[3] A.N.: This economic model proposes to realize a harmony among the interests of the state, syndicates and patronages. The state poses the right to intervene in the economic activity by diverse regulations.
[4] A.N.: It is characterized by high fiscal and cooperation between the private sector and the state, in order to fulfill some economic and social needs.
[5] A.N.: Its characteristics are: the meritocracy, lifelong employment, the competition economy. It is based on the national cohesion and solidarity.

During the last three decades, taking advantage of the global failure of socialism, the neoliberal version of the capitalism (USA and The UK) has represented the dominant economic model at the international level, significantly influenced the agenda of the governance and the reforms in the majority of the world's states, including the developing ones.

The state capitalism, on the other hand, represents a form of capitalism coordinated by the state, which does not deny the advantages of the free market. The states that practice this kind of capitalism seek to explore these advantages in order to maximize the national political power in the international arena, by contrast with the free market capitalism, whose raison d'être is the financial profit. In order to reach the goal, the state capitalism combines elements specific to the free market ideology with an active governmental role (but a discrete presence/visibility, however) in the economic management, in the orientation of the economic and strategic aims, in the elaboration of the economic policies, including innovation.

It is worth noticing that the current model of the state capitalism does not have its origin in socialism and it does not take its inspiration from that time. Different from the state capitalism specific to the former socialist regimes that were characterized by closed economies, the current state capitalism is profoundly integrated in the global economy and practices a free trade.

The state capitalism is preponderant in the fields considered strategic: the armament production, energy, security, critical infrastructure, top technologies. For instance, the state's companies have become economic giants that control important domains of the global economy and they are an essential instrument of the economic growth led by the state. Thus, the biggest 13 companies in the energy field, considering the reserves they control, belong to the governments. Saudi Aramco (Saudi Arabia), Gazprom (Russian Federation), China National Petroleum Corporation (China), National Iranian Oil Corporation (Iran), Petróleos de Venezuela (Venezuela), Petrobras (Brazil) și Petronas (Malaysia) are some of the largest. Exxon (USA), the largest transnational firm with private capital, is at the 14th place at the world level[6]. The situation is the same in the other economic fields. China and Russian Federation are leaders in the ways they support the transnational operations of their economic giants in the fields as: the defence, the production of electric energy, the export of oil and natural gas, the telecommunications, the extraction of metals and minerals, aviation. During the last years, more and more states follow their example.

In the table below are presented the main differences between the two types of capitalism.

Feature	**Free market capitalism**	**State capitalism**
Goal (stake)	Maximization of the private profit	The growth of the political power of the state
Decision-making process	Exclusive, private management	The states actively intervenes in the making of the strategic decisions
Entity that poses the property of the capital	private	The state
Firm's management	private	Both private and state
Risks taking	private	Both state and private managers
Fields of activity	All fields	Mainly, strategic fields (military, energy, telecommunications, technology)

Figure no. 1: The main differences between the two types of capitalism

[6] Ian Bremmer, "State capitalism and the crisis", 2009, URL: https://www.mckinsey.com/industries/public-sector/our-insights/state-capitalism-and-the-crisis

Not lastly, the state capitalism also represents, for the governments that adopt it, a strategy of insurance against the risk of being taken over (by legal acts of selling-buying) of the national strategic economic assets by the Western corporations, which are more mature, more experienced (including the juridical aspect) and better capitalized than the new private firms that have emerged in the developing countries starting with 1990.

As there are several models of market economies, similarly, there is not a unique model of state capitalism. There are differences, sometimes notable, between the capitalism practiced by the Russian Federations and the one practiced by China, India or Brazil. In practice, it can be noticed that of all forms of capitalism, neoliberalism contrasts the strongest with state capitalism (regardless of the particular features of the latter).

2. On what is the success of the state capitalism based?

The success of the state capitalism can be measured through: the degree of the popular support that it benefits from, the capacity to resist to external shocks, the volume of the labour force that it absorbs, the value of the strategic assets it possesses, the stability in time of the goals it follows, its contribution to the capitalization of the financial markets and even through the capacity for innovation.

In the countries that promote it, state capitalism plays an important role in the absorption of the local labour force, it gives a good resistance against the external shocks (as it could be seen during the period of the financial crisis), it guarantees the preservation of the strategic assets in the countries possession, it ensures stability of the goals along the time and has an important contribution to the capitalization of the busier mar s. A comparative look of the economies in which the state capitalism is predominant shows that it registers better results than the private capital, including in the innovation capacity.

When we analyze the preference of some governments for the state capitalism it is useful to start from studying and understanding the historical framework in which these states have been created and have developed. Both China and the Russian Federation or India represent, considering their extent and the connections they have (and in some cases the number of the native population), more than simple countries; they represent, in the first line, civilizations and cultural models. For instance, in the Confucianist culture, the state is the guardian of the people, its role in society being unquestionable. The state gives unity to the people and ensures stability of the country. These are paramount values for the Chinese society, which is characterized by a profound fear of chaos. The modern history of China is the history of the struggle for stability in the face of external pressure[7].

In its turn, Russian Federation has a long tradition of state involvement in the economic and social affairs. Historically, the Russian state was not only the quasi-permanent organizer of the economic life of the country, ensuring at the same time, some protection against the tyranny of the elite, but it has also offered a sense of national pride. The great achievements of the Russian people are strongly linked with the active and decisive presence of the state in all fields of the Russian people's life.

For these societies, from the considerations related to the historical experience, the state capitalism model is better fitted with the collective mental, which is in need of safety and the existence of a superior instance that can defend its interests. Large segments of the labour market in these countries support the state capitalism because they want firstly safety and security and only after these two are covered, they think of money.

[7] Cristopher McNally, *How different forms of capitalism are changing the global economic order*, Analysis from the East-West Center, No. 107, February, 2013.

This line of thinking is also fuelled by the global developments after the international financial crisis. More and more specialists affirm that, at present, the market cannot regulate by itself, without the state intervention, in the context in which the private firms are concerned with the maximization of the profits for themselves and not with maintaining the market disequilibria under control. In practice, there is no certitude of the fact that the interests of the private firms and those of the states (society) will be aligned, especially in the long run. The way of thinking according to which what is good for the private firms is also good for the entire society, that the former are more able than the state to appreciate what is desirable for society and what is not– this way of thinking that has prevailed in the West during the economic neoliberalism – is more and more questioned, including in these countries.

The preference of an increasing number of states for the state capitalism is based on the economic results gained by the counties with more experience in the field, other representatives being China, the Russian Federation, India and Brazil. The state companies contribute with some 80% to the financial market capitalization in China, respectively with 62% in the Russian Federation. If we refer to the impressive rhythm of China's achievements during the last two decades, we cannot but notice the role that the Chinese (government) state has played in this direction. The Chinese government has acted and acts as a complex mechanism of support and coordination of the Chinese firms activity, both state and privately owned. Actually, what the Chinese government is presently doing does not significantly differ from what the governments of developed contrived have done and are still doing albeit some nuances may still exist between them. The situation is the same in the cases of other countries. The Russian state companies operated in the energy field ensure for the Russian state a large part of the finance that is being allocated for research and development in the military field, which is considered a priority by the Russian elite in the struggle for the maintaining the country in the club of the great powers.

Another factor that contributes to the success of the state capitalism is the fact that it overplayed very well on the free market capitalism, on the investment opportunities offered by the developed countries (where the private capitalism is predominant). Referring to the factors that have contributed to the consolidation of the state capitalism, Nari Kannan suggests that this is „a product of the consumption without discernment, of the thirst for cheep goods (an allusion to the Chinese goods – a.n.) and of the dependence of the foreign oil, especially in the USA"[8]. But the phenomenon is not limited to this country.

A strong element for the state capitalism is the appearance and development of a new class of sovereign investment funds. These funds function as deposits for the surplus in the export activities and the reserves of foreign currency. States that pose great amounts of foreign currencies found taking over risks funds, with the goal of the maximization the gains from investments and, possibly, of the increasing the political influence. Further on, they use these funds to finance state companies, a fact that has attracted vehement criticism from the western governments side. These critics are fuelled by the lack of transparency as far as the goals and the real motivations for creating these funds are concerned. Western governments perceive state capitalism as a threat to the neoliberal economic order[9]. The sovereign investment funds have become important forces in the global economy, representing around 1/8 from the total global investments[10].

[8] Jim Heskett, "What is the Future of State Capitalism?", *Harvard Business School*, URL: https://hbswk.hbs.edu/item/what-is-the-future-of-state-capitalism

[9] Xing Li and Timothy Shaw 2013, *The political economy of Chinese state capitalism*, Journal of China and International Relations, Vol. 1, No.1, 2013, pp. 88-112.

[10] Xing Li and Timothy Shaw, *op. cit*.

Not lastly, the consolidation and extension of the state capitalism have been facilitated by the recent failure of the neoliberalism (on the background of the international financial crisis) in the development countries. Perhaps the current success of the state capitalism wouldn't be so obvious if it hadn't been regarded, even indirectly, by contrast with the myths that were fabricated around the private capitalism. The economic extremism practiced during the last four decades in a range of countries previously in the siege of the former Soviet Union has also contributed in a large measure to the current success of the state capitalism. For these countries, at least, the conclusion is that the neoliberal model didn't fulfil its promises; moreover, it has aggravated the economic problems, where it has been applied.

After a series of failed experiments, in countries like the Russian Federation, Chile, Argentina and in some of the East-European countries, it has become more and more evident the fact that the implementation of the free market capitalism either does not function everywhere or it doesn't function in the way predicted by its ardent supporters. In the Russian Federation, for instance, there is consent among the governmental elite and the population according to which the privatization made during 1990 have permitted to the Russian oligarchs to capture assets of the state, to gain financial and political power, which they have further exercised against the interests of the Russian state. The current elite from Moscow consider that the free market combined with the democracy has brought chaos and economic and social vulnerability in the country.

Ultimately, the model of capitalism practiced by the emergent economies should not surprise anyone, as the differences in approach among the developed and developing states can be observed also in other fields, such as security and development and they have historical roots, as we have already mentioned above. This is happening because these states (but not only them) are seeking their own role and channels of influence inside the structures of the regional and global governance. The current global situation illustrates the fact that these states have not accommodated and do not accept, in practice, the world order that has resulted after the end of the Cold War. In essence, we are talking about two different worlds, with different traditions, cultures and ways of solving economic and social problems.

3. How do the two models of capitalism coexist?

Considering a more and more evident success of the state capitalism, it is worth questioning what will happen in the societies where the predominant model is the private capitalism. The question is more pertinent as the big state companies in the emergent economies have taken under assault an important part of the economies in the West.

Several surveys have showed the diminishing popular trust in the free market and even in democracy, simultaneously with an increased interest in the alternative economic models, characterized by a higher level of the state intervention in economy, as well as in authoritarian political leaders. Surveys realized by Pew Research in more than 20 countries show that large majorities both in developed and in developing countries, disagree with the statement that „people live better in the free market economies". After the international financial crisis[11] that has broken out in 2007, in the USA, this economic model has lost much of its initial charm and capacity of attraction. According to American Enterprise Institute, the economies with authoritarian political regime have developed quicker, during the last ten years, than those of the democratic ones[12].

[11] A.N.: We consider that the therm *international* is more adecquted than global when we talk about the financial crisis starting in 2008 because this flagel does not reach the entire Globe. In fact, the emergent economies have registered spectacular economic growts, even at the top of the financial crisis.
[12] Jim Heskett, *op.cit.*

In the social field, neoliberalism has led to the increase of the inequalities in wages, both within the countries and among them[13]. The increase of inequalities has corrosive effects upon societies. It has led to a greater degree of polarisation (both inside the countries and among them), that aims at all spheres of the human life; it has enhanced the public distrust in institutions, as well as a feeling of frustration, especially that not always those who have and are able, are always the worthiest.

Not lastly, the increased inequality undermines democracy. The current wave of popular protests around the world, that tend to extend more and more and which has as main root the economic and social inequality increasingly accentuated inside the modern societies, will raise new questions for democracy. In connection it is worth noticing that although the corruption subject is replicated especially in societies from „the new democracies" (often without making connections with the source of corruption), where it has become a daily menu for mass-media, it is, however, also felt in developed societies, where the local population associates huge wealth with different acts of corruption.

More and more researchers put under question whether china can offer a model for development that can be replicated by other states, as the USA has offered through the *Washington Consensus.* Due to the historical, cultural and demographic Chinese particularities, it is difficult to deliver a clear answer. Nevertheless, regardless of the fact that the Chinese model will be considered, along the time, a good model to be followed, the success per se of China will stimulate other governments to imitate the Chinese model, perhaps trying to adapt it to their own national circumstances.

The economic links that China has with a range of states, as well as the current attitude of many western governments towards China, suggest that the Chinese political-economic model can represent an alternative to the neoliberal model patronised by the West. This alternative can aim at the socio-economic model of development, the values and the beliefs that the Western nations will embrace in the future. For the moment, it seems that the economic benefits of the cooperation with China determine the elites in some of the western countries to minimize the impact that a cleavage in the socio-economic model will play upon their societies. It seems that these elites are in line with the former general secretary of the Chinese Communist Party, Deng Xiaoping, who said that „it does not matter whether the cat is black or white, as long as it catches the mice."[14]

In these conditions, it cannot be excluded that the ascension of the state capitalism in the emergent economies will stimulate the desire of imitation in the West. Just to offer an example, in this sense, we mention that the Directorate for the companies and industry of the European Commission reflects on the need of creating *European champions* that should face competition with the increasingly stronger companies in the emergent economies. In particular, France has created, during the presidency of Nicolas Sarkozy, an investment fund, admitting that it had been influenced by China's example.

It was said that the free market capitalism is in crisis. At least for the current moment, this idea seems to us to be exaggerated, if we take into account the fact that the main economic powers in the world continue to embrace this economic model. In any case, it should be explained what this crisis is all about. In our opinion it does not regard the risk of the

[13] A.N.: For instance, in the years 1970, the CEO in the corporations earned 40 more that the modest salariers in the country. In 2007, this ratio was 400 at 1. Another example: between 1979 and 2006, the incomes of the middle clas in the USA have risen with 21%, those of the poorer segment had an increase of vcele 11%, and those of the richest 1% of the population has gone up by 256%. (Source: Paul Dobrescu, *Lumea cu două viteze*, Editura Comunicare.ro, Bucureşti, 2013.)

[14] McKay, Alonso-Fradejas, Brent, Sauer și Xu (2017) în Samuel Davis, *Hegemonic Challenge: Chinese State Capitalism and its Growing Global Presence*.

disappearance of the western capitalism, as a specific way of organizing power, economy and finance, but it can indicate the necessity of its reorganization and reconstruction in a new form – perhaps using the "threat" of the state capitalism. But the idea that this type of capitalism goes through a crisis also has another practical utility. It placed under discussion the viability of this model in the long run, considering the success registered by the state capitalism.

The current dynamics between the two models of capitalism is characterized by competition and mutual dependence. The trajectory of the state capitalism will be influenced by the possible economic measures that the governments in the developed countries could adopt, by the consumption pattern in the developed countries, but also from China and India (countries with the largest populations in the world), as well as by the capacity of the governments in the last two countries to create new employment places. The political aspects have always influenced the economic results and vice versa. The current debate with regard to the models of capitalism can represent an open lesson of political economy. The fact that some of the Western states resort to state capitalism (by doing business with it) can indicate a trend of moving towards – or adapting to – a new consensus regarding the global economic order.

4. How the two models of capitalism can collide?

Between the two models of capitalism there is a potential for conflict, that can become manifest both as far as the economic theory and practical consequences are regarded.

As far as the economic theory is regarded

The success of state capitalism has attracted critics from the side of the Western researchers. These consider that the governments that practice this kind of capitalism support (offering, thus, an incorrect advantage) their own state companies in the economic competition with the private firms from other states. At the same time, these researchers accuse the state capitalism of economic inefficiency and of promoting some political state interests.

The supporters of the state capitalism, on the other hand, consider the criticism unfounded and hypocritical, in the conditions that the states that support the free market capitalism have delivered impressive public funds in the private firms, in order for the latter not to go bankrupt as a result of the difficulties appeared on the background of the international financial crisis (to whose initiation they have otherwise massively contributed). This fact happened both in the USA and in the Western Europe. At the same time, it is argued that this economic model ensures stability, predictability, economic growth and a greater degree of social harmony. The adepts of the state capitalism consider that a deregulated market – characteristics of the neoliberal capitalism – creates socio-economic divergences and emphasizes the existing social inequalities because „it does not know either limits or moral"[15]. The market, even that deregulated, does not function objectively but it always advantages those who make up its rules, which is the powerful segment of the population.

If we are thinking that, eventually, people are interested more in the way they live and feel and less in the significance of some concepts, we can suppose that behind these positions lays a feeling of fear related to the socio-economic development model that could prevail sometime in the future rather than the simple concern for its economic efficiency.

The current discourse referring to state capitalism should be understood in the larger context of the geo-economic and geopolitical rivalry between the western bloc, led by the USA, and that Eurasian (led by the tandem China – Russian Federation). Perhaps what currently draws the attention, as far as this economic model is concerned, is less its fairness towards the private economic agents on the global market, or its efficiency, but the fact that it

[15] Thomas Piketty, *Capitalismul în secolul XXI*, Editura Litera, București, 2015.

is currently practiced by the large economies that have the force to attract other states into their orbit.

It is worth mentioning that this kind of capitalism has been practiced by countries such as The United Kingdom, Germany and Japan. In fact, the free market capitalism has its origin in the state capitalism. States as Norway, Finland or Japan are currently practicing, to some extent, state capitalism, without being criticised for that. The triggering factor of the criticism towards the state capitalism was represented by the international financial crisis; by its effects, it has induced a divergence inside the current discourse about capitalism. If during the Cold War period, the political and economic competition was carried out between capitalism and communism, at present, the political and economic game has changed: we have a competition inside capitalism, more precisely among the alternative models of capitalism. In fact, the current debate is also a reflection of multipolarity.

The current debate *private capitalism versus state capitalism* cannot be separated from the geopolitical and geoeconomic competition among the great powers consecrated and those in ascension. The current dynamics of globalization, marked by sanctions applied to the great power in ascension by the Western powers and, in general, the strategic practice engaged by the powerful economies reflects the corporatist rivalry for the control over the resources and global markets. The traditional geopolitics was based on using brutal (military) force; the new geopolitics is based more on the *soft power* (including the enormous power that the social networks exercise), using large spaces created by globalization[16].

The two models of capitalism support and cater for two distinct models: security and development. The understanding of the current discourse about the state capitalism is affected taking into account that the analysis of the links between security and geo-economy is modest in literature (including in the Western one). Although in the official discourses there is a certain precaution towards using some concepts such as *geopolitics* or *geo-economy* (for reasons related to the Nazi ideology dominant during the years of 1930, in Germany), the facts and events that have been unfolding during the last years on the world stage suggest that these links cannot be ignored without the risk of being misunderstood or misinterpreted.

As for the practical effects of the consolidation of the state capitalism...

The current polemic around capitalism does not aim at a pure theoretical discussion, but it is a reflection of the concern related to the possibility of extension at a large scale (at least regional) of a state capitalism.

The first, and the most important concern, is related to the socio-economic model for development. The current competition between the Western bloc and the Russian Federation and respectively China, is not only a geopolitical struggle between large spaces/civilisations/ cultures, as it was already suggested by many researchers, but it is also a competition between the alternative models for capitalist and financial development, in a multipolar world order in which the transnational corporatist power is the defining feature of the social organisations. This aspect is more evident at present in the case of the Sino-American rivalry and less in the case of the Russian-American rivalry. In the last case, the military vector has the trigger and traction role in the development of the rivalry. The trade war and the economic and commercial sanctions are instruments of geo-economic struggle that the West engages in towards China and Russian Federation (the choice of either one of the adversary is based on the geo-economic and geopolitical profile of the adversary, as well as the risks and vulnerabilities that using the respective instrument have for the initiator).

[16] Daniel Woodley, *Globalisation and capitalist geopolitics*, Routledge, Taylor@Francis Group, 2015.

The states with market economies are at present facing some economic, political and social challenges unmet after 1945. Until recently, the free market capitalism has established entirely on its own the global economic agenda and the desirable economic model at world level. According to this model, the market was the only institution that has established the most efficient way of allocating resources (meaning the labour force, financial capital, goods and services). The state has had only a limited role in the whole economic activity, being in turn responsible with providing the legal framework and obeying it; in general, it was concerned with ensuring the survival of the existing economic model.

The appearance of some alternative models of the economic development represents a challenge and, possibly, a serious threat for the economic model represented by the private capitalism – model predominant in the West – especially in the light of the success of state capitalism over the last two decades. It could be difficult for the private firms in the advanced economies to compete with those belonging to the state in the developing economies. In the past, the western firms were in the offensive positions; at present, their efforts are concentrated on maintaining the current market ratios than on its expansion. It is also worth noticing that in the past, they succeeded in attracting the best trained people from the local markets in the developing economies, at present, they have to compete with the largest national companies for attracting the local talents because these national companies can offer comparable wages with the ones and, moreover, they can resort to the patriotic agenda, especially in the conditions of the rebirth of the nationalist trend in more and more areas all over the Globe.

Politicians in these states, in turn, will have to face some difficult decisions, even harder that the business men. At present, it is manifested a trend of spreading of a power within the international system, from the West to the new emergent economies (mainly towards Asia), as a result of the international financial crisis (albeit this is not the only cause). On this background, these states have become more incisive in the international forums, relying also on the fact that they have received more respect and influence than at any time in their history. After the economic-financial crisis, the influence of the western politicians has diminished, as well as a result of the more intense activism of the leaders in the emergent economies.

For instance, China has gained, in the negotiations within G-20, a higher percent of vote in the International Monetary Fund. This was realised in the detriment of some Western-European states (the USA has succeeded to maintain the percent of 85% from the total votes). The activism of the leaders in the emergent economies also embraces a form of contestation increasingly vocal of the legitimacy of the Western bloc. This contestation does not come only from the side of the political leaders, but also from the side of some intellectuals in these states (mainly from Asia). These intellectuals proclaim more and more vocally the superiority of their national values and denounce the decay of the western civilisation.[17]

The dynamics of the competition between the private and state capitalism depends on the calculus that the corporatist elite in the West make for themselves, on the conclusions that they will reach regarding the perspective of the maintaining the supremacy on the Globe, China and Russian Federation towards the actions of the Western bloc. After the international financial crisis, it was obvious that the political elite in the West cannot ignore the interests of the corporatist elite in these countries. In this context, it is worth mentioning that the financial elites are mainly interested in the security of the capital. The big corporations are loyal first and foremost to their own capital and less to the states where they have the social residence.

It is necessary to correctly understand the dynamics on its way to being established between the two models of capitalism because this can have important consequences on the global economic and political stability. As long as the West did not face rivals in the economic

[17] G. Kolodko (2015), *Încotro se îndreaptă lumea*, Editura Polirom, Iași.

field, the discourse about the security was based on the military dimension and had geopolitics as a main field of confrontation. In the present conditions, with rivals whose economic force cannot be ignored, it is likely that the links between the military and the financial dimensions of security will be disclosed more and more.

As the world political order that has resulted after 1989 is questioned more and more, in the same way the world economic order is unclear. Some, including Joseph Stiglitz, the laureate of the Nobel prices for economy, states that the *Washington Consensus* is already history.

There is no doubt – the state capitalism practiced by China, India, Russian Federation or Brazil represents a competitive economic force at the global level and a challenge, from the political viewpoint for the Washington Consensus. As it was seen in the decisions of G-20, following 2008, these countries challenge more directly the international financial architecture than previously done. In order to understand the nature and the logic of the state capitalism challenge to neoliberalism we have the Cold War period to look at. The current state capitalism has adapted to many of the principles of the free market capitalism and it is well integrated in the global economic system. As such, the state capitalism is not situated outside the neoliberal economic order and it does not intent to replace it, but it wants to maximize the political power for those who practice it. The firms in these countries are not always led by the governments in their countries. In the Russian Federation, for instance, there is a strong private sector, especially in the retailed field, constructions, food, wireless communications, and auto and even in the metal extraction. The essential distinction is that the state saves to itself the right and the role to intervene in the important economic affairs. Nevertheless, this aspect can also be noticed in the neoliberal market economies or in the social market economies. Only two examples in this sense: the USA did not permit the selling of the national firm Unocal (that operates in the energy field) to China, for reasons of "national security"; as well as that, Germany does not agree to sell to the Chinese firms some of the assets, either national or belonging to the European Union, that it considers to be strategic (also particularly, in the energy).

Conclusion

As far as we are concerned, we consider that any prognosis regarding the economic model dominant in the future is premature and hazardous. Those who argue that the state capitalism is inefficient and unsustainable ignore the success that it has recently registered in a number of increasing states, including the desire of some advanced states to benefit from the support offered by this economic model. On the other hand, those who argue that the future belongs to the state capitalism are in a rush, minimizing the fact that most economically and financially powerful states practice the free market capitalism and they are aware of the risks of giving up to this economic model. We have all seen the influence that the big corporations in the West exercised on the governments in their countries in even on the global economic order, over the past years.

Based on the arguments presented in this paper, we consider that the perspective approaching the competition between the free market capitalism and the state capitalism as a zero-sum game is wrong. A realist and balanced look has to admit that a variety of models of organizing capitalist production and markets can coexist. The capitalism was, from its very beginning, and still continues to be heterogenic, even inside the bloc made up from the developed countries.

In shaping the future world order, the financial aspects could be even more important than the traditional geopolitics, in the conditions of the USA supremacy still uncontested in the

military field. For the Western elites, the financial aspects (the security of the financial flows, the marginal rate of the corporatist profit) are no less important than the military one, considering the direct link existing between the financial perspectives of the large corporations and the political and social dynamics in these countries.

By contrast with the traditional geopolitics, which is characterized by the logic of the national security, the current capitalist geopolitics is characterized by the security of the ruling class. By the last concept we understand, at first, ensuring a profit ratio (the marginal rate of the profit) that ensures the ruling elite maintains and continues the financial and political power. The competition for the financial domination on the Globe could be a more important triggering factor for future crisis or conflicts than the geopolitical claims of China or the aggressive behaviour of the Russian Federation towards its neighbours.

BIBLIOGRAPHY:

1. KOLODKO, G., *Încotro se îndreaptă lumea*, Editura Polirom, Iași, 2015.
2. MCKAY, Alonso-Fradejas, BRENT, Sauer and Xu (2017) in Samuel Davis, *Hegemonic Challenge: Chinese State Capitalism and its Growing Global Presence*.
3. MCNALLY, Cristopher, *How different forms of capitalism are changing the global economic order*, Analysis from the East-West Center, No. 107, February 2013.
4. PIKETTY, Thomas (2015), *Capitalismul în secolul XXI*, Editura Litera, București.
5. XING, Li and SHAW, Timothy, The political economy of Chinese state capitalism, *Journal of China and International Relations*, Vol. 1, No.1, 2013.
6. WOODLEY, Daniel, *Globalisation and capitalist geopolitics*, Routledge, Taylor@Francis Group, 2015.
7. BREMMER, Ian, 2009, URL: https://www.mckinsey.com/industries/public-sector/our-insights/state-capitalism-and-the-crisis
8. HESKETT, Jim, "What is the Future of State Capitalism?", *Harvard Business School*, URL: https://hbswk.hbs.edu/item/what-is-the-future-of-state-capitalism

THE ROMANIAN DEFENCE INDUSTRY IN THE INTERNATIONAL ARMS SALE MARKET'S COMPETITION

Crăișor-Constantin IONIȚĂ, Ph.D.
Researcher at the Centre for Defence and Security Strategic Studies
within "Carol I" National Defence University, Bucharest, Romania.
E-mail: ionita.constantin@unap.ro

Abstract: *There is a fierce competition in the international arms sale market regarding the export of very high-tech and sensitive defence material. For some developed countries, like Russia, Greece, Italy, France, Sweden, the manufacture and sale of armaments represent a substantial percentage of their GDP and a possibility to grow their income and wealth. At the same time, because of the different research and development levels of advanced technologies in the production of defence capabilities, like multi-purpose platforms, unmanned systems, robotics, nanotechnology, artificial intelligence/learning machines, there is a huge discrepancy between American defence industry and the European one. This is really true when you consider the dependence of European industrial companies from their American counterparts. This dependence has obliged some European defence companies to establish bilateral or multilateral collaboration agreements to survive in the field of armaments export. For the Romanian Defence Industry, the discrepancy is even higher than Western similar companies, considering its reliance on old technologies, lack of specialists and research institutes, and acquisition of majority of its military equipment from the US. There is little interest from both the Government and the MoND to invest in national defence companies to buy their military products, which have lower technology incorporated and low performance equipment.*

Keywords: *Defence Industry; Forces of the National Defense System (FSNA); Pan-European companies; advanced technology; developed industrial and technological defense base (DTIB); unmanned systems; artificial intelligence/machine learning; nanotechnology; technological discrepancy.*

Introduction

One important national resource available for the development of military capabilities is the defense industry. Along with human, financial and logistical resources, the defense industry provides the technological part, as well as the research, development and innovation one of developing those defence capabilities approved at political level and stipulated in the sectorial strategic documents.

At the national level, the resources needed to develop defense capabilities are made available through the Government programs and are a distinct part of the defense budget. At NATO and EU level, the respective resources are provided from the Common Budgets and Member States' contributions.

According to the provision of the National Law no. 232/2016, the national defense industry is that branch of the national industry that includes companies officialy enroled in the register, with either state or private capital, which have the available technical, technological, organisational and management resources necessary for assuring and supplying institutions

and structures of the Forces of the National Defense System (FSNA) or other countries with military, sensitive and strategic products and/or related services.

In some developed countries, there is no defense industry branch of the national industry, but the production of armaments is with large private companies, mostly civilian (USA, UK, France, Germany etc.), gathered in so-called Military-Industrial Complex (MIC) - an informal alliance of national Armed Forces, the armaments industry and the ministries/departments of the respective governments.

In order to understand the economic leverage and, more importantly, the fierce competition taking place in the international armaments market, this paper will analyze how the defense industry participates in the development of national and collective/common defense capabilities, as well as what the Romanian political leaders should do to make the national defence industry a competitive actor at the European and global levels.

1. The international arms sale market and its main actors

The armaments industry, also called the arms trade, is a global industry that manufactures and sells weapons and military technology both nationally, for the state's defense, as well as internationally, to states that do not have their own production capabilities. National or multinational companies that produce weapons and provide logistics or operational services in the military field are also called arms salers/dealers, defense contractors or the military industry.

Worldwide, military spending reached $ 1.822 billion (bn.) in 2018[1], which represented a decline from the 1990s, when defense spending was 4% of GDP. However, there has been a 5.5% increase in arms trade over the past five years as a result of global events, especialy in Eastern Europe, North Africa and the Middle East (MENA), as well as in South-East Asia (see fig. 1). Also, according to data provided by Stockholm International Peace Research Institute (SIPRI), in 2018 the largest exporters of military equipment were the USA, Russia, France, Germany and China, out of a total of 67 states exporting small arms, aerospace and naval systems and security technology, including cybe. According to the same organisation, the largest importers were Saudi Arabia, India, Egypt, Australia and Aleria (out of a total of 155 importing countries). Recently, there has been an increase in arms exports from the United States, France, Israel and China, while the one from the Russian Federation decreased significantly. Weapons are sold mainly in areas of open conflict.

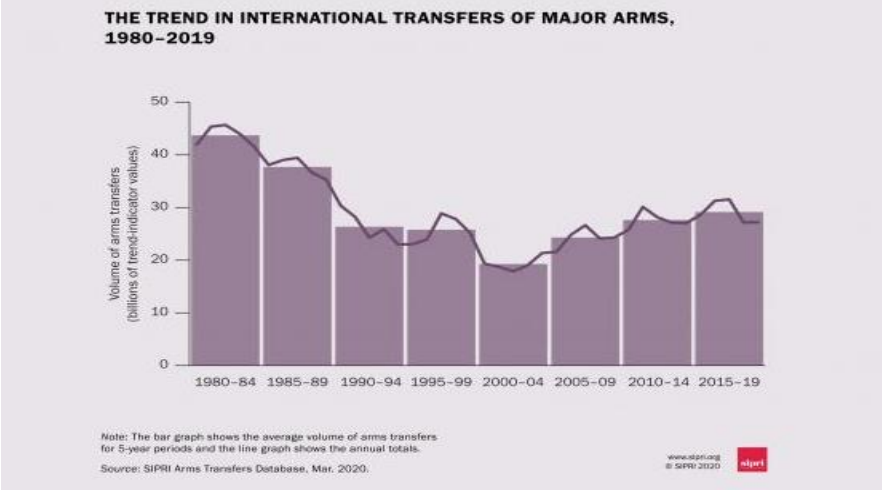


Figure no. 1: Trends in the International Arms Sale Market between 1980 – 2019
**Source: www.sipri.org*

[1] ***, „Trends in International Arms Transfer, 2019 – Fact Sheet", *The Stockholm International Peace Research Institute (SIPRI)*, Solna, March 2020, p. 1.

There is a global tendency to decreese the importance and impact of a global enabler that controls arms exports in the international arms sale market, through non-proliferation, control and prohibition treaties, established and signed by member states. The main treaties/agreements refer (but are not limited) to: the Geneva Protocol on the Non-Proliferation of Chemical and Biological Weapons (1925), the Treaty on the Exploitation of Outer Space (1967), the Convention on the Prohibition of Biological Weapons (signed in 1972 and entered into force in 1975), Missile Technology Control Regime/MTCR (1987), Chemical Weapons Ban Convention (signed in 1993 and entered into force in 1997), Ottawa Anti-Personnel Mine Ban Treaty (signed in 1997 and entered into force in 1999), the new START Treaty between Russia and the USA (signed in 2010 and entered into force in 2011), Arms Trade Treaty (signed in 2013 and entered into force in 2014). In addition to the positive contribution that the international community has made to the non-proliferation and control of the arms race, the measures taken to ban it or its lack/inefficiency have led to increasing global arms trafficking and the cessation of some effecient treaties/agreements like : Nuclear Non-Proliferation Treaty (signed in 1968 and entered into force in 1970), Underwater Nuclear Test Ban Treaty (signed in 1971 and put into operation in 1972), Anti-Ballistic Missile Treaty (signed in 1972 and ceased in 2002, because of the USA withdrawal), SALT I (signed in 1972, and entered into operation in 1997), which was replaced by SALT II (signed in 1979 and never entered into force), the INF Treaty (signed in 1987 and canceled in 2019, following the withdrawal of both Russia and the USA), START I (signed in 1991 and finalised in 2009), being replaced by START II (signed in 1993, and terminated in 2002, because of the Russia withdrawal), as well as the Treaty for Conventional Forces in Europe/CFE (signed in 1990 and entered into force in 1992). Following the US withdrawal, the Open Skies Treaty (signed in 1992 and entered into force in 2002) is partially applicable.

According to the well-known Business Insider Magazine, from Germany, curently there are 25 largest arms manufacturers in the World, either national or multinational[2]. Their classification is based on the arms sale figures and the longest period of time they have dominated some important domains of the international arms sale market. Of course, the majority of them are coming from the US - *Lockheed Martin Corp.* (44.9 bn. USD, the biggest arms producer from the world, being specialised in global security and defence, as well as in aerospace); *Boeing* (26.9 bn. USD, one of the well-known producer of airships, missiles, satelites and communication systems); *Raytheon Technologies Corp.* (23.8 bn. USD, the world biggest producer of guided missiles, being also specialised in military and civilian armaments and electronic systems); *Northrop Grumman Corp.*(22.3 bn. USD, the world biggest small arms producer, being also specialised on defence systems and aerospace); *General Dynamics Corp.*(19.5 bn. USD, produces defence and aerospace products); *United Technologies Corp.*(7.7 bn. USD, in April 2020 fusioned with Raytheon to form a multinational concern, specialised on aviation engines and space systems); *L3 Technologies Inc.*(7.7 bn. USD, specialsed on communications, information and surveillance systems); *Huntington Ingalls Industries* (6.8 bn. USD, being specialised on military ships and tehnical solutions); *Honeywell International Inc.*(4.6 bn. USD, a multinational concern that produces aerospace systems and provides technical services); *Leidos* (4.3 bn. USD, produces software for military, as well as aviation, biomedical research and information technology); *Textron* (4.1 bn. USD, an industrial concern with many armamments companies); *Booz Allen Hamilton* (4 bn. USD, being specialised on military technology); and *General Electric* (3.8 bn. USD, builds engines and propulsion systems).

[2] Sophiei Ankel, "From Lockheed Martin to Airbus: These are the 25 largest arms manufacturers in the world", *Business Insider Magazine*, 16 November 2019, URL: https://www.businessinsider.com/these-are-worlds-25-largest-arms-manufacturers-in-the-world-2019-11, accessed on 07.07.2020.

Others represents the EU or its Member States, like: *BAE Systems Inc.* (from the UK, 22.9 bn. USD, specialised in mutinational defence and security, as well as aerospace technology); *Airbus Group* (a Pan-European company, 11.2 bn. USD, specialised on aerospace); *Thales Group* (from France, 9 bn. USD, being specialised on NATO electronics and the production of aerospace, transport, and security systems), *Leonardo* (from Italy, 8.8 bn. USD, being specialised on aerospace, defence and security); *Rolls-Royce* (from the UK, 4.4 bn. USD, being specialised on engines, aviation, and navigation); *Naval Group* (from France, 4.1 bn. USD, specialised on shipbuilding and submarines); and *Rheinmetall* (from Germany, 3.4 bn. USD specialised on mobility and air industry).

There are also arms companies coming form Russia - *JSC Concern VKO „Almaz-Antey"*(8.5 bn. USD, a big producer of armaments and small arms); *PJSC United Aircraft Corp.*(6.4 bn. USD, specialised in aerospace and defence systems); *United Shipbuilding Corp.* (4.9 bn. USD, specialised on shipbuilding, as well as on submarines); and *JSC Tactical Missiles Corp. – АО Корпорация Тактическое Ракетное Вооружение/КТРВ* - (3.5 bn. USD, being specialised on armaments production).

There is one big armaments company that belongs to Japan, *Mitsubishi Heavy Industries*, with a sale figure of 3.5 bn. USD, which is specialised in engines and aviation industry. However, in Asia the newly available data suggest that China is "the world's second-biggest arms producer, behind the United States and ahead of Russia[3]". Because of in the international arena's huge tensions caused by the appearance and spread of Covid-19 andd the luck of transparency in providing right data and information from the Chinese authorities, SIPRI has omitted to include Chineze companies amongst the biggest international arms sale producers. This, Aircraft and avionics group *Aviation Industry Corporation of China* (*AVIC*, 20.1 bn. USD in 2017) whould rank as the sizth largest arms producer, while land systems-focused *China North Industries Group Corporation* (*NORINGO*, 17.2 bn. USD) would place eight in sales. The other two companies it looked at are *China Electronics Tehnologies Group Corporation* (*GETC*, 12.2 bn. USD) and *China South Industries Group Corporation* (*CSGC*, 4.6 bn. USD).

The analysis of the production and, especially, sales activity of these large multinational corporations shows that their turnover is influenced by the extremely high prices of military products, especially aerospace, ballistic missile and air defense systems warships and submarines, but also advanced technologies. This desideratum led to their classification as presented above.

2. European defence industry

EU policy on the use of Member States' defense industries in the development of defense programs (EDTIBs) is based on the aggregation of experiences, technologies and production capacities that they can bring in their colaboration on armaments production and the development of military capabilities in this multinational context. But, inside the EU, the national interest of Member States is higher than the multinational development of military and civilian capabilities through common projects proposed by the EDA under the Pool & Sharing and PESCO initiatives. Their desire to involve their own defense industries more than other states in these projects led to conflictual discussions and missunderstandings on the multinational development of those capabilities. Some Member States have differing views on the involvement of European defense industries, while others embrace a "common European

[3] ***, "China has world's second-largest arms industry, think tank estimates", *Reuters*, 27 January 2020, URL: https://www.reuters.com/article/us-china-arms-production/china-has-worlds-second-largest-arms-industry-think-tank-estimates-idUSKBN1ZP0UE, accessed on 21.09.2020.

purchasing" mentality, being interested in maintaining an open defense market, in which non-member states, such as the USA, have access.

In fact, we have three groups of states in the EU struggle to establish a European defense industry policy linked to the Common Security and Defense Policy (CSDP). The first group, which includes, among others, Italy, Poland and Sweden, wants to maintain a close transatlantic link, demanding that any commitment to EDTIB to not affect cooperation with the US. A second group comprises those countries being specialised in niche capabilities and which, although not having a developed industrial and technological defense base (DTIB), continue to play an active role in the European supply chain and in the innovation group/research. The last group represents the states that already concentrate the production of European defense systems and is led by France and Germany. The two states will play a leading role in defining the role of EDTIB in European Defense, especially in the development of future major European programs on the implementation of Future Fighter Jet Systems (FCAS) and Main Ground Fighter Aircraft (MGCS)[4].

For France, competition for armaments production and sales is vital and related to DTIB, being considered an integral part of the CSDP. As early as August 2019, the idea of President Francoise Macron is to achieve "European strategic autonomy", in order to achieve Europe's sovereignty[5]. That is why the few large French companies have global trends, promoting both domestic collaboration (eg Nexter - Lacroix), but also at European level (eg the Franco-German group KNDS, which will produce the European battle tank/EMBT, amphibious protected tracked vehicle/ APTV and MGCS). In addition to the *Thales Group* and *Naval Group*, which were presented in the previous chapter, France also has the following important companies in armaments production: *Nexter* (part of the KNDS Group, specialised in the production of complete defense systems for the Land Forces, artillery pieces and ammunition); *ARQUUS* (specialised in armored and special purpose vehicles); *Sofema* (artillery systems and machine guns); *CNIM* (assault bridge systems, unmanned vehicles, amphibious boats, electronic surveillance systems and cyber security); *PGM* (individual weapons and ammunition); *Orbitico* (GPS and navigation systems); *Aubert & Duval* (parts of missiles, artillery pieces and individual weapon pipes); *Safran S.A.* (engines and propulsion for tactical missiles, drones and UAVs, navigation systems and equipment, electronic systems); *Etienne Lacroix Group* (vehicle survival systems, zonal protection systems, pyrotechnic means, aerial, naval and terrestrial training systems).

Germany broadly shares France's vision of European integration and the future political role of the EU, wishing Europe to have its own effective defense industry. Although the German defense industry is considered to be a key component of European security, Germany nevertheless wants to maintain the transatlantic link for the construction of defense equipment[6]. As a result, German armaments companies within the DTIB are national and highly diversified on certain products specific to national defense and foreign markets, with a variety of domestic and international collaborations. In addition to *Rheinmetall Defense*, which was presented earlier, Germany also has: *Krauss-Maffei Wegmann GmbH & cCo. KG* (member of the KNDS Group, participates in the realization of armored vehicles on wheels and tracks, research systems, anti-aircraft and artillery, simulators, CIS systems and weapon stations with remote-controlled research and observation equipment); *ThyssenKrupp* (a

[4] Daniel Fiott, "The CSDPin 2020: the EU's legacy and ambition in security and defence", *European Union Institute for Security Studies (EUISS)*, Bielot, Bruxelles, 2020, p. 126.
[5] *Ibidem*, p. 127.
[6] Bastian Giegerich, "Armament and Transatlantic Relationships: The German Perspective", *ARES Group Comment*, no. 45, 22 October 2019, URL: https://www.iris-france.org/wp-content/ uploads/2019/10/Ares-Group-45-1.pdf., accessed on 16.07.2020.

German conglomerate specialised in the production of engines, ships and submarines, chemical compounds, power generators, fighter jets and land vehicles); *Diehl Diesel* (high-tech defense equipment, missiles and intelligent ammunition, as well as ground-based air defense systems); *Hensoldt* (field observation and evaluation systems, detection and identification, radars, electromagnetic and optronic warfare systems, long-range surveillance systems); *Mercedes-Benz* (heavy tactical and logic vehicles for the Land Forces); *FFG* (armored vehicles); *Eurospike GmbH* (portable AA and anti-tank missile systems); *Dynamit Nobel Defense* (portable anti-tank missiles3); *Heckler & Koch GmbH* (small arms); *Sig Souer GmbH & Co. KG* (small arms); *Hensoldt* (observation and firing systems, situational awareness systems, reconnaissance and surveillance systems, electronic protection systems); and *Artec GmbH* (armored vehicles).

Italy is ranked in the top 10 arms exporting countries in the World in the land, air and naval fields. Italian DTIB operates both nationally and in European projects (the first European unmanned combat vehicle - UCAV). In addition to *Leonardo SpA*, which was presented earlier, Italy also produces and sells weapons through the following companies: *CIO Iveco - Oto Melara* (an internal collaboration consortium, established in 1985, to manufacture tanks and armored vehicles); *Iveco Defense Vehicles* (armored vehicles, as wekk as tactical and logistical vehicles); *Vega Holster* (individual tactical equipment for infantry); *Benelli Defense* (small arms); *Fiochci Ammunition* (small arms' ammunition); *Simmel Defense* (artillery ammunition, missiles and SADs).

Spain's defense industry is very heterogeneous, containing both micro-firms and large multinational concerns, being concentrated on aerospace, naval (surface ships) and electronic sectors. The Spanish Industrial Defense Strategy is based on the development and consolidation of the industrial sector, as well as on the internationalisation of companies through the export of military equipment. But the implementation of this strategy is difficult - only through multinational participation in European projects, such as: *Santa Bárbara Sistemas* (member of SBS-GDELS, produces armored vehicles, logistics vehicles, SIAC launcher, bridge systems and artillery ammunition); *Expal* (launchers, specialised vehicles for Enginner and Special Forces, as well as ammunition for NATO); *Urovesa* (combat vehicles); *Excavator* (parts and propulsion systems for tanks and armored vehicles); *Installation* (small arms); *Indra Sistemas S.A.* (3D air defense radars, Silver BMS command-control system, ES ground radar systems); *Navantia* (SERT surveillance, exploitation, research and shooting systems).

Poland, the most developed country from the former communist block, had to fiercely fight to penetrate the European and International Armaments Market. In recent years, it managed to increase its defence industry involvement, in most cases collaboratively through European projects, but also at national level, by creating a Polish Armaments Group (PGZ), to produce land platforms, ammunition, major electronic systems, helicopters, combat and torpedo systems. The main Polish companies in the defense industry are: *AMZ* (armored vehicles); *Fabryka Broni „Łucznik" Radom* (small arms); *Jelcz* (armored combat and special purpose vehicles); *HSW* (rocket launchers, command-control vehicles, engineer vehicles); *Concept* (logistics vehicles); *Rosomak SA* (armored vehicles); *Pitrodwar* (radar and fire control systems); *WB Group* (communication, command and control systems, fire control systems, intelligent ammunition systems, burst ammunition); *Dezamet SA* (mortars and related ammunition); *PCO SA* (individual and vehicle optoelectronic equipment); *Nitrochem* (explosives and artillery ammunition); *Teldat* (command-control and management systems); *Zaklady Mechaniczne Bumar-Labedy S.A.* (tanks and logistics vehicles).

Sweden demonstrates a real and developed export activity with defense materials, as well as the ability to create, produce and support a variety of sophisticated weapon systems. It

maintains its national sovereignty at the critical points of its armament policy, focusing on aerospace products, underwater systems, cybernetics, automobiles and telecommunications, autonomous vehicles and robotics. Among the major armament companies, it is worth mentioning: *Saab Bofors Dynamic* (C-IED and electronic systems, ground-based AA defense systems, missiles, UTAAS system for tank and AA, ammunition, as well as special purpose vehicles); *Akers Krutbruk* (vehicle protection, mine protection and FDI, active defense systems); *Scania CV AB* (trucks for heavy transport); *Volvo Defense* (engineering equipment and heavy transport vehicles); *TAIGA AB* (personal protective equipment); *SCANJACK* (zonal demining systems); *Nammo* (artillery, anti-tank ammunition and small arms); *BAE Systems AB* (armored vehicles and tanks, artillery systems).

Greece uses its defense industry both to protect its security hotspots and to increase its domestic product, being an adept of the collaboration at the national level, but also of interacting with foreign partners. The main companies in the defense industry are: *EODH* (anti-ballistic, demining and IED means of protection, as well as individual protective vests); *EAS* (small arms and related ammunitions); *THEON* (optoelectronic and tactical means); *Kioleides* (military trucks and transport vehicles); *ELVO* (tanks and armored vehicles, special pourpose vehicles); *Intracom Defense* (communication and electronic systems, radio systems, terrestrial surveillance systems, unmanned systems); *HDVS SA* (parts and subassemblies for tanks and armored vehicles); *VALPAK SA* (military camouflage systems); *SSMART S.A.* (integration of combat systems); and *METKA S.A.* (integration and manufacture of parts and subassemblies).

The Czech Republic has a dynamic and technologically developed defense industry in the aerospace and terrestrial sectors, being more export-oriented. In addition to the airline *Cesnna Textron Aviation* (with a long tradition in aircraft production of short courier Turbo Stationair HD and medium courier Skycourier, parachute Caravan, Grand Caravan EX for SRI), Czech DTIB has specialised, recently in the export of small arms and ammunition, repair and maintenance services for armored vehicles, as well as the production of prototypes and experiments. Among the Czech armament companies it is worth mentioning: *Excalibur Army* (tanks, combat vehicles and artillery pieces); *M4* (tactical equipment); *argun.cz* (ballistic systems); *Ceska Zvrojovka* (small arms); *FK Brno* (small arms and ammunitions); *STV* (combat vehicles, artillery pieces, small arms and related ammunitions); *Arm Svos* (armored vehicles); *Tatra Mountains* (transport and logistics vehicles); *VOP CZE* (maintenance services and auro technical repairs); *KARBOX* (containers and car chases); *OMNIOPOL* (electronic means and portable AA systems).

The Netherlands has a dual defense industry, serving both the military and the country's economy. It comprises several large companies and several medium and small enterprises for supporting foreign customers, such as: *Damen* (the only shipping company that produces warships, patrol boats, landing craft, auxiliary vessels and training ships); *Thales Netherlands* (ground surveillance radars and vehicle communications system); *Van Halteren Defense* (vehicle parts, simulation and training systems, ground systems parts); *Rheinmetall Defense Netherland B.V.* (armored vehicles); *Dutch Defense Vehicle Systems* (military vehicles); *DSM* (ballistic shields, helmets and vests); *Defenture* (multi-role vehicles and air transport tactical vehicles); *GEMCO* (command, control and communication systems); *CRYSTAL COMPANY BV* (Crystal armor); *Deba Trucks* (Anaconda vehicle).

Trans-European defense companies have been set up to demonstrate the internationalisation trend of DITB in Europe. In order to reduce fierce competition in the International Armaments Market, to attract and ensure the expertise of companies specialising in niche products, parts and accessories or to provide services in specific areas of defense, as well as to reach consensus in approving multinational European projects, It was set up so-

called trans-European cooperation groups to implement the approved Pan-European initiatives and to be able to cope with international arms trade competition. In addition to the *Airbus*, which was described in the previous chapter, we can also mention: *MBDA* (a multinational group formed by Airbus, Bae Systems and Leonardo, specialised in the production and sale of anti-tank missiles and MMP, AA missile systems, radar and command-control systems on vehicles, AA systems, as well as special purpose vehicles); *Eurosam* (another multinational group created by MBDA France, MBDA Italy and Thales for the production and sale of Ground-Based Air Defense systems); *KNDS* (the association of the Franco-German companies Nexter Defense Systems and KMW for the production of the European battle tank EMBT).

Romania is also present in the European DTIB, but only through low-tech armaments products, such as small arms and related ammunition or the provision of services. Lately, Romanian decision-makers are making efforts to create a competitive defense industry on the European market, especially by concluding cooperation agreements with renowned companies in Europe, such as Thales in France, Rheinmetall in Germany or MOWAG in Sweden, in order to attract state or private companies to participate in some European projects to be included in the Romanian defense capabilities, such as PIRANHA IIIC and PIRANHA V. The Romanian defense industry will be presented in the next chapter.

3. Romanian defence industry

If there is a substantial gap between the American and European defense industries, especially in terms of incorporating high-tech systems in the development of pan-European initiatives, the major technological gap between Romanian and Western state-owned companies is disastrous. This is also due to the dependence of the defense capabilities being developed at national level on the Russian and American technology.

The technological gap mostly consists of: the existence of aging technologicies and less prepared human resources; the state industry's dependence on traditional products exports, with outdated technologies; political factor involvement that inhibited profound changes and often altered, through politicisation approach, the quality of the managerial act; the fragility of the state-private defence industry partnership, the latter often playing the role of subcontractor for foreign companies and providing assistance in the integration of new equipment on existing platforms; the lack of predictability of state funding coherent multi-annual endowment programs, which affected both state and private industry; the practice of too ambitious or unrealistic requirements in relation to resources, which led to the endowment of the Armed Forces with excessively expensive products and questionable interoperability; military research underfunding status and the quasi-non-existence of public-private cooperation in the field; the lack of an inter-institutional strategy to determine a coherent process of research and development of security technologies.

There is also a legal aspect for not having an efficient and competitive national defence industry – the old and, sometimes, obsolete normative framework at the national level. This is the case of some Governmental Decisions (HG) and Emergency Ordinances (OUG), like: OUG no 57/2002 for scientific research and technological development, approved by Law no 324/2003; HG no 1266/2004 for approving the metodological norms of contracting, financing, monitoring and evaluating projects from reaserch-development sectorial plans; OUG no 158/1999 for establishing the export and import regimes for strategic products, approved by Law no 595/2004; OUG no 202/2008 for implementing international sanctions at national level, approved by Law no 217/2009; OUG no 189/2002 for compensating operations regarding aquisition contracts for defence, public order and national

security needs, approved by Law no 354/2003; ANCEX Order no 849/2012 for approving metodological norms for OUG no 158/1999; HG no 414/2004 for approving the functioning regulation of the defence resources' priority and allocation system; HG no 1094/2011 for approving the List of military products under the export and import regimes; OUG no 119/2010 for control regime of double-use products[7].

Thus, as stated by Mr. Viorel Manole, the Executive Director of the Romanian Business Association of the Military Technique Manufacturers (PATROMIL): "since 1990 no major national project has been developed, able to equip the Armed Forces and ensure the export of products manufactured in Romania, which incorporate advanced technology.[8]" Therefore, we must not forget that one of the characteristics of the International Arms Sale Market is the competitiveness imposed by high requirements. In addition, orders are fluctuating, depending a lot on political issues, either internally (such as forecasting the 2% of GDP spending, during 2016-2026 period, for the purchase of military equipment and weapons necessary for modernising and transforming the Romanian Armed Forces 2026) or externally (some influential partner states are particularly interested in supporting the sale of their own military equipment, and, as such, these topics are often on the agenda of bilateral political meetings).

Starting with 2016, there was a positive movement in the legal framework regarding armaments production and aquisition aspects, through the approval of the Law no 232/2016 for the national defence industry, Laws no 98 and 99/2016 for public and sectorial aquisitions, Law no 100/2016 for leasing services and works, as well as the HG no 0534/2015 for approving the List of economic operators and defence producer capacities.

The Romanian defence industrial system is mostly based on state own armaments companies and a few private ones, specialised on builging spare parts and providing special services. The main Romanian state supplier of defence technologies and services is *the National Company for Military Technique (ROMARM, 92.9 mil RON in 2019)*, with a constant presence in over 50 markets from all around the world. It has 15 subsidiaries: *Arsenal Resita S.A.* (different types of cannons and howitzers); *Bucharest Mechanical Fcatory* (*UMB*, research, design, production, repair and upgrading of armores vehicles); *Carfil S.A.* (production of NATO-compatible armaments and ammunition and provide service and maintenaince services for armaments); *Cugir Arms Factory* (production of infantry weapons and machine guns); *Cugir Mechanical Plant* (produce NATO-type ammunition); *Fagaras Powders Plant* (the only manufacturer of high-powered explosives and solid propellers); *Electromecanica Ploiesti* (the only producer of rokets and missiles); *Metrom S.A.* (military manufacturer of ammunition components); *Mija Mechanical Plant* (producer of anti-tank grenades, military grenades, products for maintaining public order); *Moreni Mechanical Plant* (producer of amphibious armored vehicles 4x4, 6x6 and 8x8); *Pirochim Victoria* (military powders); *Plopeni Mechanical Plant* (artillery ammunition); *Tohan S.A.* (artillery ammunition, warheads for missiles and pyrotechnic elements); *Sadu Mechanical Plant* (producer of infantry ammunition); and *UPS Dragomiresti* (artillery ammunition, aviation bombs, explosives)[9].

---

[7] ***, "Industria de aparare", the Minister of Economics, Energy and Business' URL: http://www.economie.gov.ro/aparat-propriu/economie/industria-de-aparare, accessed on 21.09.2020.

[8] Viorel Manole, "Reziliența, achiziții și infrastructura militară, axe de mobilitate", a PPT Presentation at *the International Scientific Conference of Experts SECDEF 19*, organised by the Romanian Reserve Officers Association (AORR) and the Military Technical Academy (ATM) „Ferdinand I", 7-9 November 2019, Bucharest.

[9] ***, "Defence and Security Market Report, Romania, June 2018", *Virginia Economic Developing Partnership (VEDT) - International Trade*, EasyLink Business Services, Brussels, 2018, pp. 16-18.

Apart from ROMARM there are other several important state arms companies - *the Military Equipment and Technologies Research Agency* (*METRA*, part of Armaments General Directorate, for scientific research and technological development); *AVIOANE S.A. Craiova* (23.4 mil RON, specialized in advanced trainer aircraft manufacture, repair and overhaul of military aircraft); *IAR S.A.* (152 mil. RON, the leading Romanian aerospace company); *IOR S.A.* (17 mil. RON, producer of sighting and aiming apparatus for infantry, artillery and armored vehicles); and *ROMAERO S.A.* (46.5 mil. RON, integrates aero structure manufactecturing with maintenance and repair of civil and military transport aircraft) - and private armaments producers, like*: AEROFINA S.A.* (10.5 mil. RON, research, production and testing of military equipment); *AEROSTAR S.A. Bacau* (356 mil. RON, regional leader in aviation manufacture and civil aircraft maintenance); *AEROTEH S.A. Bucharest* (64 mil. RON, design, development, production/repair, assembly, service and marketing for hydraulic and pneumatic equipment in the field of aviation and gas distribution); *CONDOR S.A. Bucharest* (18 mil. RON, manufacturer of parachutes and military fight equipment); and *TURBOMECANICA S.A. Bucharest* (83 mil. RON, manufacturer of jet engine components and assemblies)[10].

Romania spent, in 2019, 4.9 billion dollars for its Armed Forces, according to the SIPRI report, which means an increase of 17% compared to the previous year. Thus, Romania is among the countries with the highest increase in military spending in the last 10 years (2010-2019), ie 154%, being surpassed by Lithuania (232%), Latvia (176%) and Bulgaria (165%)[11].

The question that arises here is what percentage of the defense budget has been directed towards making acquisitions nationwide? We know that most of the budget was spent to purchase external capabilities, such as: American multi-role aircraft F-16 (18 aircraft aquired from Portugal, with 250-300 million euros), the French corvette program Gowind 2500, the American anti-missile defense system Patriot (only this cost, in 2017, 3.9 billion euros for 7 systems), the integrated missile system SHORAD / VSHORAD (2.1 billion euros), the modernisation of the T22 frigates (also with the French from Naval Group), armored vehicles PIRANHA IIIC and V (227 Swiss armored vehicles, which cost 900 million euros), Iveco transport and special purpose vehicles (942 wheeled transport platforms in various configurations, worth 1.015 billion lei), Harris and Panther communication systems, Exocet MM40 coastal missile batteries (with the trans-European MBDA Group, worth 164 million euros - they will also equip French corvettes with the same missile system), the long range missile system M-142 HIMARS (3 systems from the American company Lockheed Martin, worth 1.5 billion euros), combat helicopters, C4ISTAR systems[12].

There has also been a positive change in the attitude of political and military decision-makers towards the involvement of the national defense industry in developing military capabilities necessary for the Romanian Armed Forces by 2026. Thus, the construction of four corvettes and modernisation of existing fregates were discussed and accepted with the French *Naval Group* at the *Constanța Shipyard*, together with the establishment of a naval maintenance and training center for corvette crews, also in Constanța. Meanwhile, the big

[10] *Ibidem*, pp. 19-20.
[11] Andrei Luca Popescu, "Marii cheltuitori militari ai lumii. Cum a ajuns România să dea pe Armată cu 150% mai mulți bani, față de acum 10 ani", *Free Europe Broadcast*, 27 April 2020, URL: https://romania.europalibera.org/a/marii-cheltuitori-militari-ai-lumii-romania-armata-bani/30579481.html, accessed on 21.07.2020.
[12] *Ibidem*.

loser of this contract, the *Damen* Dutch company, built a corvette for the Pakistani Navy in the *Galati Shipyard*, which is managed by them, together with the one in Mangalia[13].

Another big European company, Airbus Helicopters, developed in 2016, an industrial partnership in Brașov, in the aeronautical sector, with the IAR Ghimbav company, for the construction of the multi-role helicopter H215M SUPER PUMA[14]. Same thing happened with the Swiss Mowag GmbH company, part of the GDELS concern, which started, on November 6, 2019, the construction of 227 TIRT 8x8 PIRANHA V armored vehicles at the Bucharest Mechanical Factory (UMB)[15]. Also, the Italian Iveco Defense Vehicles S.p.A. company signed, on 30 March 2020, an agreement with the Office for Compensation for the Acquisition of Special Equipment (OCATS), in which 600 military vehicles will be made in Romania, at a factory established through mutual agreement (contract worth 813 million RON). The German EuroSpike GmbH company started at S. Tohan S.A. Factory two projects regarding technology transfer activities to the Romanian factory and export activities, amounting to 2.62 million euros.

The arrival of the Italians from Beretta to the Plopeni weapons factory for the construction of a new assault weapon of the Land Forces is still being negotiated since last year. Also, there are discussions with the Elbit Systems Ltd. company from Israel and Thales from France on the placement of orders to the Romanian companies Elmet International SRL, A-E Electronics SA, respectively Thales Systems Romania S.R.L., of an estimated value of 29 million dollars.

A very positive element of the Romanian economical policy in the last period was the change in the process of acquiring combat equipment for major programs, like C4ISR, corvettes and 8x8 transport vehicule. In the new approach the procedure invoked for choosing a manufacturer is centred on the security interest, based on art. 346 of the Founding Treaty of the EU. This proves that the Ministry of National Defense shows more determination in trying to encourage and support the participation of the national industry in the major endowment programs that the Romanian Armed Forces have initiated. In this regard, an important step was the modernisation of the legal framework, by adopting the Law no 232/2016 on the national defense industry, which specifies that the protection of national defense interests, including the essential interests of national security, is achieved, among others, by increasing the competitiveness of economic operators to meet Romania's defense interests by stimulating investments in the national defense industry, scientific research, technological development and innovation and by involving the national defense industry in integrated logistics support activities of military equipment. It is worth emphasising that the law mentions that the Ministry of Economy, as the responsible institution that manages the problems of the defense industry, "supports the participation of the national defense industry, regardless of the form of ownership[16]" in carrying out the endowment and modernisation programs of institutions within the Forces of the National Defense System (FSNA), thus trying to ensure, at least from a legal point of view, an equal status between state and private companies in Romania. Reference is also made to the capabilities and areas of activity of the defense industry, which are of strategic importance at the national level and represent fundamental security interests of the country, such as: production and manufacturing capabilities of powders and explosives, production capacities and performing maintenance for military equipment, production and

[13] George Marinescu, "Corvetele, între aranjamentele lui Naval Group și realitate", *Bursa Newspaper*, 2 March 2020, URL: https://www.bursa.ro/corvetele-intre-angajamentele-lui-naval-group-si-realitate-43390937, accessed on 21.07.2020.

[14] As per the site www.airbus.com, accessed on 21.07.2020.

[15] As per the site www.gdels.com, accessed on 21.07.2020.

[16] ***, "Legea nr. 232/2016 privind industria națională de apărare, precum și pentru modificarea și completarea unor acte normative", published in *the Romanian Official Monitor*, no. 972 from 5 November 2016, art.6, pct. (5), lit. g).

manufacturing capabilities of ammunition and infantry armament and capabilities to perform and integrate command-control systems[17].

It is worth mentioning here that the perspective of including private companies in the national defense industry has changed, demonstrating how the Government finally understood the necessity of a balanced and integrated approach to the two components of the national industry - the state and private ones. Unfortunately, the practice of congesting the aquisition process in the last month of the year continues, even if there are well-defined funds at the beginning of the year. But the cumbersome system of procurement procedures opted for or the prolonged bureaucratic procedures at the Government level are those that affected the earlier acquisitions. As a result, we consider that, if rapid legislative measures are not taken to accelerate the process of procuring combat equipment, in accordance with the programmes assumed by the Ministry of National Defense and validated at the Supreme Council of National Defence (CSAT) level, there is a major risk that the Romanian Armed Forces will not be able to spend those funds provided for endowment, as happened between 2015 and 2017.

To this end, in 2016 the Ministry of National Defense drew attention that "insufficient funds and lack of budget predictability are the factors that affect any action taken to establish and optimise defense capabilities, appreciating that only, by adopting laws that ensure a certain budgetary predictability [i.e. the achievement of a predictable multiannual financing] and rhythmic allocation of necessary funds can assure the success of finalising, on time, the essential endowment programmes". Moreover, the respective law should put into practice the provisions of the Memorandum on measures to streamline the endowment of the Romanian Armed Forcea and increase the involvement of the national defense industry in finalising those major programmes, as approved by CSAT Decision no. 11/24.11.2016.

*
* *

The importance of national defence industry for both the development of military capabilities neceesary for the rrespective Armed Forces and the increase of economic development and social wealth is paramount. It represents in itself a well-defined national resource and enabler of the national defence and security strategic objectives that can be used also to warrant the common European security and Allied collective defence.

In order to have a well developed defence industry, the government should take all necessary measures to make it more efficient and competitive on the international arms sale market. Otherwise, the industrial policy of relying on imports would be detrimental for the economic development of the country, as well as for the national defence.

The first step of becoming efficient and competitive on the international arms sale market consists in taking "a slice" from the European major projects. This could happen either as a lead or framework nation inside a group of Member States, or as arranged bilateral or multinational industrial partnerships with big European armaments companies. Of course, the competition is so difficult, and it is almost imposible to overthrone France and Germany from the EDTIB's projects.

Romania needs to take big steps to cover the huge industrial disparity, not only in incorporating advanced technology in the manufacturing of its products, but in its national industrial development strategy. In this respect, some major investments in research and strengthening cooperation between national security institutions and state-owned companies, on one hand, and private companies in Romania, on the other hand, open up new perspectives for the efficient use of public money. As a result, in addition to modernising the legislative framework, it is necessary to implement a National Research and Development Programme

[17] *Ibidem*, art. 5.

within the new strategy, which allows private investments in research and development to have some warranties about the final involvement of the state in funding those national projects after being validated and tested. Involvement of the Romanian defense industry in public-private partnerships with the defense industries at the national level and abroad (especially with NATO and EU countries) and creating the necessary conditions for conducting beneficial offset contracts in the acquisition/modernization of military equipment – especially on the research-development-innovation dimension (RDI) for the creation of new equipment/technologies for military use, is an essential prerequisite for its revitalization/ refurbishment and reduction of the competitiveness gap.

An important step in ressurection of the national defense industry in the race to win local, European and even global markets is the recent economic recovery plan announced by the Government in early July, as well as the prudent investment of the 79,9 billion euros, approved by the EU for Romanian participation in European projects, within the multiannual budget 2021-2027 and the post-covid economic recovery package, adopted at the Brussels Summit, between July 16-20.

BIBLIOGRAPHY:

1. ANKEL, Sophiei, "From Lockheed Martin to Airbus: These are the 25 largest arms manufacturers in the world", *Business Insider Magazine*, 16 November 2019, URL: https://www.businessinsider.com/these-are-worlds-25-largest-arms-manufacturers-in-the-world-2019-11
2. FIOTT, Daniel, "The CSDPin 2020: the EU's legacy and ambition in security and defence", European Union Institute for Security Studies (EUISS), Bielot, Bruxelles, 2020.
3. GIEGERICH, Bastian, "Armament and Transatlantic Relationships: The German Perspective", *ARES Group Comment*, no. 45, 22 October 2019, URL: https://www.iris-france.org/wp-content/uploads/2019/10/Ares-Group-45-1.pdf
4. MARINESCU, George, "Corvetele, între aranjamentele lui Naval Group și realitate", *Bursa Newspaper*, 2 March 2020, URL: https://www.bursa.ro/corvetele-intre-angajamentele-lui-naval-group-si-realitate-43390937
5. POPESCU, Andrei Luca, "Marii cheltuitori militari ai lumii. Cum a ajuns România să dea pe Armată cu 150% mai mulți bani, față de acum 10 ani", *Free Europe Broadcast*, 27 April 2020, URL: https://romania.europalibera.org/a/marii-cheltuitori-militari-ai-lumii-romania-armata-bani/30579481.html
6. ***, "China has world's second-largest arms industry, think tank estimates", *Reuters*, 27 January 2020, URL: https://www.reuters.com/article/us-china-arms-production/china-has-worlds-second-largest-arms-industry-think-tank-estimates-idUSKBN1ZP0UE
7. ***, "Legea nr. 232/2016 privind industria națională de apărare, precum și pentru modificarea și completarea unor acte normative", in the *Romanian Official Monitor*, no. 972 from 5 November 2016.
8. ***, "Defence and Security Market Report, Romania, June 2018", *Virginia Economic Developing Partnership (VEDT) – International Trade*, EasyLink Business Services, Brussels, 2018.
9. ***, "Trends in International Arms Transfer, 2019 - Fact Sheet", *Stockholm International Peace Research Institute (SIPRI)*, Solna, March 2020.
10. www.airbus.com
11. www.economie.gov.ro/aparat-propriu/economie/industria-de-aparare
12. www.gdels.com

REGIONAL SECURITY IN THE BLACK SEA – SOLUTIONS FOR THE FUTURE: THE SECURITY, STRATEGIES AND FORCES BALANCE

Mihai PANAIT
PhD Candidate, Rear Admiral, Naval Forces Staff
E-mail: mihai.panait@navy.ro

Ion ROCEANU, Ph.D.
Colonel (r.) Professor, "Carol I" National Defense University
E-mail: iroceanu@adlunap.ro

Abstract: *The post-pandemic period of COVID-19, in addition to profoundly changing international relations (especially globalization), brought a new perspective on the relationship among the concepts of regionalization, regionalization of security, new strategies and doctrines (to support them in the conditions of changing the level of operation imposed by COVID-19) as well as the type of new military equipment that will be found in the multi-annual procurement plans. The nature of the threats acquires a new nuance with the appearance of this pandemic and soon puts in front of the politico-military decision-makers, new reference points that will bring to the level of these days the fundamental documents (strategies, planning directives, procurement programs) that will support budgetary planning for the coming decades, research and innovation (to develop new platforms, sensors, and weapons with a small number of combatants), and new aspects of diminishing international and regional cooperation in favor of unilateral action. From now on, the new dimensions of the defense budget will have to contain other elements adapted to the COVID-19 fight.*

Keywords**:** *Regional security; strategies; international relations; globalization and isolationism.*

Introduction

The balance of power is the focus of geostrategy and is vital for international stability. It is almost impossible to give a definition of power or to identify a comprehensive theoretical approach that addresses all aspects of power balance. In international relations, the balance of power is a key concept that presents the state as concerned by power, especially military power, in an environment where risks and threats operate and which is considered to be the most important rational actor, which makes decisions based on calculations of the most advantageous cost and using existing information and resources.

Thucydides explicitly stated that the Peloponnesian War was not caused by the problems declared by the belligerents, but by *"the growing power of the Athenians and the fear it caused in Sparta"*[1]. For realists, this is a classic example of the impact that the anarchic structure of international politics has on the behavior of state actors and the balance of power. Kenneth Waltz, one of the founders of neorealism, describes the Spartans' motivations for war with Athens when he claims that *"having the two coalitions, the greatest success in attracting members of the opposing party could tempt the other to risk a pre-emptive war, hoping for an unlikely victory,*

[1] Thucydides, *The Landmark Thucydides, a comprehensive guide to the Peloponnesian war*, Ed. R. B. Strassler, New York, Touchstone, Rockefeller Centre, 1998, 1.75.

before the differences between them increase significantly"[2]. Waltz argues that *"powerless states, if they were free to choose, would be attracted to weaker states or alliances because of threats from the strongest side (...)*[3]*"*. Thus, Thucydides states that in the Peloponnesian War, the smaller states of Greece considered strong Athens as a tyrant and weak Sparta as liberators. This view of international politics (also known as structural realism) emphasizes that the structure of the international system and the place of a state in this system are more important for interstate relations than the internal functioning or culture of each state[4].

In addition to being used to support the principles of structural realism, Thucydides is often considered an exponent of *"classical realism",* according to which the anarchy of the international system is not caused by the system itself, but a product of the individual characteristics and aspirations of each state. Thucydides, through his discourse in the Mytilene debate, is seen as an exponent of the view that human nature is *"self-interested and unconstrained by any higher moral laws,"* a vision that leads to the belief that "*everything and everyone is a mean, a tool, which has to be justified in terms of its usefulness and which must achieve its objectives*[5]*".* Applied in the theory of international relations, it means that *"fear and distrust of other states provide the reason for the rise of power by waging wars to subdue those who, when the time comes, will seek to subdue the strong"*[6].

I used Melian's dialogue to argue that Thucydides believed that "*Athens, with the power and ability to rule an empire, was forced to do so, due to the laws of nature, which dictate that the strong dominate the weak, that you must rule wherever you can, that your self-interest does not contradict the considerations of justice and that others will rule over you if you fail to control them*[7]". In addition to fear, Thucydides also acknowledged that in search of glory, wars could be provoked[8], and for these reasons states will always try to increase their power, thus altering the balance of power to the detriment of other states.

The balance of power was a key concept for Europeans. Metternich and his contemporaries, reviewing the Post-Napoleonic *Concert of Europe,* felt that the balance of power was the only way in which states, supported by geography and their natural resources, population morale, national expansiveness, and consuming much of their economic, military and diplomatic capacity to impose its will and authority on neighboring states, could coexist in peace. If a state gains a politico-military advantage over its neighbors, it will be tempted to exert its influence on the power instruments of neighboring states, to threaten with the use of force and, last but not least, to expand. This tendency to impose one's will through military power, diplomacy to other states was maintained throughout the twentieth century, even though the balance, almost perfect before the First World War, was not enough to prevent its outbreak.

Spykman argued that the fundamental element in the balance of power was instability. The balance always tended to deviate from equilibrium, because of the components of balance, namely, the states themselves, did not know, with any degree of certainty, how much

[2] K.N. Waltz, *Theory of International Politics,* S. I. Columbia University, Ed. Long Grove, Waveland Press, Boston, 1979, p. 126.
[3] *Ibidem*, pp. 127-128.
[4] Tim Dunne, Brian C. Schmidt, *Realism*, p. 162, http://www.academia.edu, accessed on 22.08.2017.
[5] David Boucher, *Political Theories of International Relations: From Thucydides to the Present,* Oxford University Press, New York, 1998, p. 29.
[6] *Ibidem*, pp. 30-31.
[7] *Ibidem*, p. 34.
[8] Thucydides, *The Landmark Thucydides, a comprehensive guide to the Peloponnesian war*, Ed. R. B. Strassler, New York, Touchstone, Rockefeller Centre, 1998, 1.75.

power was on the other scale, and therefore it was desirable not a balance, but an excess of power. *"Uncertainty, the lack of measuring instruments, attempts to increase the relative power, all turned the calculations upside down. When the balance has been disturbed; the consequence was war*[9]*"*. Without this instability, the implications of the unbalanced powers are much less threatening. Just as the industrialized nations of Eurasia are not concerned with balancing the overwhelming power of the United States[10], America should not be concerned with the game of balance in Eurasia. Many of today's richest states choose not to build huge armies[11].

Spykman described in the *United States and the Balance of Power*[12] the anarchic character of world politics infused by a strong geopolitical realism. In the absence of a world governmental authority (as we observed during the pandemic when countries took all self-defense measures), the primary interest of all states is self-preservation or survival. *"The fundamental objective of the foreign policy of all states,"* he wrote, "is to*" preserve territorial integrity and political independence*[13]*".* This international anarchy has, as a result, a relentless power struggle among states resulting in a security imbalance in the region. "*The struggle for power*", he explained, "*is identical with the struggle for survival, and the improving of the relative position of power becomes the primary goal of states' domestic and foreign policy. All the others are secondary because in the last resort only the power can reach the objectives of the foreign policy*[14]". Instead, policymakers, depending on the level of power of the state to which we refer, must be concerned with the regional or global balance of power. "*Experience has shown"*, he wrote, "*that there is more certainty in a balanced power than in a declaration of good intentions"*[15]. Spykman also noted that there have been few cases in history in which states have tried to limit or constrain their power. Instead, he explained, "*states are only interested in a balance of power that is in their favor. Not a balance, but a generous margin of power in their favor is their goal.*" The balance of power, in Spykman's opinion, is not a static phenomenon, but a continuous change in the relations between the great powers. *"The margin of security of one country",* he wrote, "*is the margin of danger for the other, and therefore the alliance must be met by counter-alliance and armament by counter-armament, in eternal competition for the fight for power. This has been the case in all periods of history*[16]".

In the field of international relations, the balance of forces was first defined at the Vienna Congress on June 9th, 1815. At this congress, the concept of balance of forces was defined for the first time as a result of the military imbalance caused by Napoleon[17]. To restore its economic and military capacity, Europe needed a longer period of recovery and

[9] Edgar S. Furniss Jr., "The Contribution of Nicholas John Spykman to the Study of International Politics", *World Politics*, Vol. 4, No. 3, April 1952, p. 391.
[10]Layne Christopher, "The Unipolar Illusion: Why New Great Powers Will Rise", *International Security*, Vol. 17, No. 4, Spring 1993, pp. 5-51.
[11] H. J. Mackinder, *Democratic Ideals and Reality. A Study in the Politics of the Reconstruction by the Right Honorable Sir Halford J. Mackinder*, National Defence University Press, Washington, 1942, p. 9.
[12] Nicholas J. Spykman, *America's Strategy in World Politics: The United States and the Balance of Power*.
[13] Nicholas J. Spykman, op. cit. p. 17
[14] Nicholas J. Spykman,op. cit. p. 18
[15] *Ibidem*, p. 20.
[16] Nicholas J. Spykman, op. cit. pp. 20-21
[17] Stella Ghervas, "Congresul de la Viena şi pacea europeană", Historia, accessed from https://www.historia.ro/sectiune/general/articol/congresul-de-la-viena-si-pacea-europeana, on October, 05th, 2020

clarification of the concept of balance of power, primarily by Castlereagh (England), Metternich (Austria) and Tsar Alexander (Russia)[18]. This Congress created new tools and perspectives for the development of international relations, especially the Concert system, and gave the first meaning of the term balance of power, namely, that this refers to a process in which no nation or alliance will become predominant.

The definition of equilibrium is very complicated, as it is in the dictionary, namely as that "*property of a system of forces or other actions which have as a result zero effect and, consequently, does not change the state of the body or the phenomenon on which it is exercised[19]".* Thus, balance is not the zero result of two forces (or in case of war/conflict, the zero-sum game), but is rather a simultaneous action, of several factors (including the desired level of security, the strategies we want to be implemented, and the necessary forces to meet the objectives of the state in the area of responsibility) so that a system can result in the lack of effects that would damage the system (or to security), defined in the notion of *the zero-sum game.* It is very difficult, in the case of politico-military decision-makers, to establish the proportion of state's power instruments that address this aspect of the balance between the level of security (which we want to be achieved at the national and regional level), the strategies needed to identify the lines of development to achieve this goal, and last but not least, the necessary armed forces.

1. Current considerations of the equation security-strategies-forces

Recently, NATO redefined *security* as: *"The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion, terrorism and damage, as well as against loss or unauthorized disclosure".*[20]

The EU does not define *security* but seeks to clarify and shape it by defining its strategic objectives. The EU Strategy for a security union[21] emphasizes that "*Security is a cross-cutting issue that .... addresses many policy areas* through which we must ensure *all the necessary connections to build a genuine security ecosystem and a global framework for our security policies which must always be fully based on our common values"*[22]. At the Black Sea and Balkans Security Forum Conference I attended this year, the Prime Minister of Romania emphasized that *"NATO and the US commitment to Europe's security remain fundamental considerations of the European Union's foreign and security policy"*[23].

[18] Bogdan Antoniu, Mihai-Rudolf Dinu, *Istoria relaţiilor internaţionale în secolele XIX-XX*, Ministerul Educaţiei şi Cercetării,2005, accessed from http://hiphi.ubbcluj.ro/studii/Public/File/cursuri/suporturi_conversie/Relatii-internationale.pdf, on October 05th, 2020

[19] Dexonline, https://dexonline.ro/definitie/echilibru accessed on September 17th, 2020

[20] AAP 6, *NATO Glossary of Terms and Definitions (English and French)*, edition 2018, p. 112, https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600, accessed on 16.01.2019.

[21] EU Security Union Strategy: connecting the dots in a new security ecosystem, *accessed from* https://ec.europa.eu/commission/presscorner/detail/ro/ip_20_1379, on 22 October 2020.

[22] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, accessed from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN, on 22 October 2020.

[23] Diana Zaim, September 4th, 2020, Calea Europeană, *Ludovic Orban, discurs la "Black Sea and Balkans Security Forum": Puterea economică a UE, adevărata forță de atracție a proiectului European", accessed from*

In the same area, but much more restrictively, the EU is trying to identify the place of security as a common need for the well-being and prosperity of the EU. The term *security* was a term ignored for a long time in international relations, especially since in post-December Romania this term had a fateful connotation, which the Romanian people were not prepared to accept, and the state was still reluctant to use it in defense policy. The neglect of the term *security* was explained by Buzan in *People, States and Fear*[24] suggesting five possible explanations, as follows: the difficulty of the concept, the apparent overlap between the concept of security and power, lack of interest in security by various critics of realism, security think-tanks are too busy to keep up with new developments in technology and politics, and last but not least, policymakers find the ambiguity of *"national security"* useful. However, these explanations seem inconclusive if we were to compare the term national security with that of the armed forces, political, financial, diplomatic, and legal. Nevertheless, the term security gains a lot in weight but also in ambiguity when the subject to which security refers is not known, the subject to which it refers is not identified, i.e. to whom we must protect ourselves, what are the values to be defended and how much security is needed to ensure a minimum of security for a nation[25].

From a legal point of view, the only national definition of security is found in Law 51/1991[26], as follows: *„(...) by the national security of Romania is meant the state of legality, balance, and social, economic, and political stability necessary for the existence and development of the Romanian national state as a sovereign, unitary, independent, and indivisible state, the maintaining of the rule of law, as well as the climate of unrestricted exercise of the fundamental rights, freedoms and duties of citizens, according to the democratic principles and norms established by the Constitution"*[27]. President of Romania, in the foreword of National Defense Strategy[28] (NDS), does not give a clear definition of the concept of security, but emphasizes that this is a process related to its responsibilities, which must be "*built on fundamental values and benchmarks, the expression of consensus and national effort common"* and to be *"designed and implemented with the citizen as the final beneficiary"*[29].

---

https://www.caleaeuropeana.ro/ludovic-orban-discurs-la-black-sea-and-balkans-security-forum-puterea-economica-a-ue-adevarata-forta-de-atractie-a-proiectului-european/ on 22 October 2020.

[24] Barry Buzan, Department of International Studies University of Warwick, 1983, *People, States and Fear: An Agenda For International Security Studies in the Post-Cold War Era*, pp 6-9, accessed from https://www.academia.edu/4780500/People_States_and_Fear_An_Agenda_For_International_Security_Studies_in_the_Post_Cold_War_Era_Barry_Buzan, on 09 October 2020.

[25] David A. Baldwin, *The concept of Security, Review of International Studies*, 1997, 23 5-26, pp. 5-17, accessed from https://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf, on 09 October 2020.

[26] *Legea nr. 51/1991privind securitatea națională a României*, republicată în 2014, art. 1, http://www.dreptonline.ro/legislatie/legea_51_1991_securitatea_nationala_romaniei_republicata.php, accesat on 05 October 2020.

[27] Dreptonline, *Legea nr. 51/1991 privind securitatea națională a României*, republicată în 2014 (Law no. 51/1991 on the National Security of Romania), art. 1, accessed from http://www.dreptonline.ro/legislatie/legea_51_1991_securitatea_nationala_romaniei_republicata.php, on October 05th, 2020.

[28] Administrația Prezidențială, *Strategia Naţională de Apărare a Ţării pentru Perioada 2020-2024 "Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări" (Presidency, The National Defence Strategy of the Country for 2020-2024. "Together for a Sure and Prosperous Romania in a World Marked by New Challenges)*, Bucharest, 2020, accessed from https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_ Aparare_a_Tarii_2020_2024.pdf, on October 06th, 2020.

[29] *Ibidem*, p. 4.

From the three definitions, we notice that, in the case of the EU and Romania, security is a state of well-being at all levels, while for NATO it is an action aimed to fulfill the actions of defending its own interests[30]. But, in all cases, *security* is *"a multi-dimensional concept, based on the relationship security - prosperity - rule of law - democracy - identity, the balance between state and individual as beneficiaries of national security, integrated security management and the idea security community"*[31].

States, in the current conditions of economic and social crisis and the fight to reduce the effects caused by the pandemic, must be further supported by Non-Governmental Organizations, Intergovernmental Organizations, the judiciary system, the mass-media (through opinion-makers) and the civilian population, to return to equilibrium.

2. The balance of security, strategies and forces in the context of the pandemic

In my opinion, we can draw a parallel between the relationship of the concepts of *security*, *strategy and military capabilities*, on the one hand, and, on the other, the Clausewitzian trinity of *people – government – army*, given that security refers primarily to that human being, the state, the system to be safe from any risk, the government is one of the main actors involved in strategic planning and sets the main directions of development, and force, as long as we refer to the military dimension of security, can be easily equated with the armed forces.

Every historical stage has been characterized by a certain type of war. But, like the previous stages, the period during the fight against COVID-19 and post-pandemic will certainly be influenced by the issue of sustaining state security and sovereignty. The virus can affect the power instruments of the state and can diminish part of the operational capacity of an army that will be forced to fight under adverse conditions given the omnipresence of this virus. In this context, even if the security threat is a biological one, Clausewitz's statements in *On War* remain particularly valid concerning the chameleon-like property of war (of conducting military action) and its ability to change the shape, thus gaining an advantage on the battlefield[32]. The famous strategist determines the elements of the strategy, as follows: "*The causes that determine in the strategy the use of the war can be divided into moral, physical, mathematical, geographical and statistical elements"*[33]. The vast majority of strategies have been thought on these grounds, but there is a lack of the element defined by this virus. I believe that politico-military decision-makers should consider, in the future, when re-evaluating security strategies and doctrines that describe how to use the force, limitations, and risks posed by the pandemic. In a crisis or war situation, the virus cannot be considered a rational actor, nor any mathematical and statistical element, thus contradicting the Clausewitzian elements of defining the war within the strategy.

---

[30] Tiberiu Tănase, Mircea Stan, *Puncte de vedere privind reforma legislativă a sistemului de securitate naţională a României*, accessed from https://www.mapn.ro/publicatii/2017/infosfera/infosfera_2_2017.pdf, on October 05th, 2020.

[31] Administrația Prezidențială, *Strategia Naţională de Apărare a Ţării pentru Perioada 2020-2024 "Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări" (Presidency, The National Defence Strategy of the Country for 2020-2024. "Together for a Sure and Prosperous Romania in a World Marked by New Challenges)*, Bucharest, 2020, accessed from https://www.presidency.ro/files/userfiles/Documente/ Strategia_Nationala_de_ Aparare_a_Tarii_2020_2024.pdf, on October 06th, 2020, p. 7.

[32] Carl von Clausewitz, *Despre Război*, Antet Press, 2006, pp. 87-88.

[33] Carl von Clausewitz, *op. cit.*, p. 76.

For the Euro-Atlantic future, the balance among security, strategy, and forces, presents some considerations that are connected with the past, the present but with an emphasis on a fresh vision of development prospects on the future of the Black Sea region and Europe. The central principle of the scientific foray in this paper is that of the balance between security, strategy, and forces that can be the key to stability and prosperity in Europe and can be the basis for a new regional security architecture.

Analyzing vulnerabilities and risks to security, prosperity, and peace, in particular, is an important step. Fragile or unstable states, organized crime, terrorism, drug trafficking, interstate conflicts, the proliferation of weapons of mass destruction and emerging technologies, competition for resources, population growth, and last but not least pandemics are risks and vulnerabilities that we need to face, to look for and to identify solutions.

One of the most important aspects is the development of democracy inside but also in the vicinity of its borders, creating the foundations for raising the standard of living and eliminating borders. Stability and security remain issues that require increased attention for neighboring states. These elements demonstrate the determination of the European Union, first and foremost, to try to identify solutions to the specific problems of the regions as a whole, but also of each country, including by implementing the timetable for financial assistance for all countries[34].

The period after the outbreak of COVID-19 pandemic, in addition to profoundly changing international relations, especially globalization, brought a new perspective on the relationship among the concepts of regionalization, regionalization of security, new strategies and doctrines (supporting them under the conditions of changing the level of readiness and interoperability imposed by COVID-19) as well as the type of forces to be acquired in the coming years. The emergence of this pandemic will move the center of gravity of the analysis of politico-military analysts and planners to bring to the present day the fundamental documents (national security strategy and subsequent strategies) that will support budget planning for the coming decades, pandemic research and innovation (to develop new platforms, sensors, and armaments, with a decreased number of combatants on board) as well as new aspects of diminishing international and regional cooperation in favor of unilateral action. From now on, the defense budget will have to contain other elements adapted to the COVID-19 fight, the economy will have to find the levers to readjust, to avoid a major financial and economic crisis and to survive this impact, and the legislation in force will it must identify new packages of rules, standing operating procedures, best practices, definitions and laws to eliminate the effects of the pandemic by the all institutions involved.

3. The impact of the pandemic on strategies and planning

The long-term effects of the COVID-19 pandemic on global security but also in the Black Sea region will produce new in-depth analyzes of riparian countries in the context of maintaining an acceptable ratio of operational plans and readiness of forces. With the advent of the virus, the readiness level of forces of many states has been diminished, producing major changes in providing security compared to the levels that have been planned, in areas of strategic interest or with multiple alterations from the legality of freedom of navigation or the

[34] Larson, Eric V., David T. Orletsky, and Kristin J. Leuschner, *Balancing Strategy, Forces, and Resources: Lessons for the Current Defense* Review. Santa Monica, CA: RAND Corporation, 2001, accessed from https://www.rand.org/pubs/research_briefs/RB73.html, at September, 20th 2020.

provisions of the United Nations Convention on the Law of the Sea, UNCLOS III[35]. The aircraft carrier Charles de Gaulle during the execution of the mission in the Foch Operation[36] had the combat capability affected as a result of the illness with COVID-19 of about half of the crew (more than 600 sailors)[37]. The USS aircraft carrier Theodore Roosevelt, during the execution of missions in operations in the Philippine Sea[38], identified as positive more than 1000 crew members[39]. The Commander of the US Forces in Europe has ordered the cessation of training activities for a US-led exercise in Europe to limit the number of illnesses among US troops[40]. Australia canceled its largest land troop biennial exercise, Hamel Exercise, and nor did send ships and troops to the RIMPAC Exercise, conducted by the US Indo Pacific Command[41]. All of these forces had diminished or even canceled the readiness level. COVID-19 put in front of military planners a situation that had not been taken into account before. Now, the role of military analysts is to determine the areas that need to be reassessed, given that this type of threat has proven to reduce the level of training and action during operations.

Next, we will try to identify what a defense strategy is. The specialized literature describes it as the art and science (at the same time) of developing and coordinating the DIME instruments of national power, to which are added the legal, financial, research, and development and informational fields, to fulfill its objectives and interests that contribute to national security[42]. A defense strategy aims are to communicate the Government's strategic vision at the national and international levels, to support the President in strengthening foreign policy, and to create an inter-ministerial and inter-governmental consensus. It is well known that the main approaches to evaluating a strategy are "*top-down*" or "*bottom-up*". The process of balancing *security, strategies, and forces*, which involves multiple actions on the part of each subordinate subsystem, is very sensitive to be adjusted in the sense that the sudden balancing of a single element can produce major side effects. For these reasons, the bottom-up approach is fully justified, although it has a major shortcoming, the planning and development process is lengthy.

The strategy is the tool that substantiates the action of analysts at the politico-military level, supported by the SWOT analysis, so that the state can ensure the desired level of security. The strategy, based on the analysis of *strengths* and *weaknesses*, determines the level of security we want to ensure and, as a result, the necessary military forces. Without a strategy

---

Convenția Națiunilor Unite asupra dreptului mării – United Nations Convention on the Law of the Sea – UNCLOS.

[36] Xavier Vavasseur, USNI News, *French Carrier Strike Group Begins 'Foch' Deployment*, January 23, 2020, accessed from https://news.usni.org/2020/01/23/french-carrier-strike-group-begins-foch-deployment, on October 09th, 2020.

[37] Anita Hawser, *Defence Procurement International*, *Coronavirus Strikes French Naval Vessel*, 16 April 2020, accessed from https://www.defenceprocurementinternational.com/news/chemical-biological-radiological-and-nuclear/coronavirus-on-board-french-aircraft-carrier-charles-de-gaulle, on October 09th, 2020.

[38] Xavier Vavasseur, Naval News, *Theodore Roosevelt, Nimitz Carrier Strike Groups Operate Together In Philippine Sea*, June 23rd, 2020, accessed from https://www.navalnews.com/naval-news/2020/06/theodore-roosevelt-nimitz-carrier-strike-groups-operate-together-in-philippine-sea/, on October 09th, 2020.

[39] Sam LaGrone, USNI News, *Carrier Theodore Roosevelt COVID-19 Outbreak Investigation Complete, CNO Now Reviewing Report*, accessed from https://news.usni.org/2020/05/27/carrier-theodore-roosevelt-covid-19-outbreak-investigation-complete-cno-now-reviewing, on October 09th, 2020.

[40] Anita Hawser, *Coronavirus Strikes French Naval Vessel*, *op. cit.*

[41] Sam Bateman, The interpreter, *Safety of life at sea: Covid-19 and naval operations*, 20 April 2020, accessed from https://www.lowyinstitute.org/the-interpreter/safety-life-sea-covid-19-and-naval-operations, on 09th October 2020.

[42] Dictionary of Military and Associated Terms. S.v. "*national security strategy*." Retrieved October 8th, 2020 from https://www.thefreedictionary.com/national+security+strategy and https://dexonline.ro/definitie/strategie.

that analyzes the geopolitical situation and identifies political, military, financial, and diplomatic constraints, strong and coherent leadership cannot be created, national/regional interests cannot be promoted and foreign policy cannot be clearly defined. Depending on the international geopolitical context and the relations among states or alliances, existing risks and threats, and national interests, the objectives proposed by the strategy are subsequently detailed through a set of strategic guidelines to be followed to achieve them. Depending on these paths, the state's instruments of power (DIME) and, implicitly, the necessary level of military forces will be used. The degree of security obtained depends on the concordance and homogeneity of the objectives set by the strategy and the instruments of power available to that actor. In my opinion, a strategy, to be relevant, must be built on *threats* (depending on the relations between neighbors or states in the region) and *opportunities* (achieving security objectives according to the foreign policy parameters of other states).

Changes in the international environment and in the nature of threats and risks to the security of EU and NATO countries, as well as the resizing the amounts of GDP for defense, the fight against the pandemic, will lead to an increased intensity of research and innovation in the military, with a focus on unmanned systems technology. The new changes in the structure of risks and threats to Romania's security, as highlighted in the *National Defense Strategy*[43], have put before analysts and politico-military decision-makers the need to develop the *culture of security of citizens*[44].

Regarding the implementation of the strategy, the Supreme Council of National Defense approved the document for the application of the NDS, including the Implementation Plan, the Strategic Defense Analysis, and the White Paper on Defense. The main objectives of the implementation plan are to monitor the elaboration of subsequent strategies, action plans, and other programmatic documents developed by public institutions with attributions and responsibilities in the field of national security, according to specific needs and limitations. The strategic analysis of the defense, with a horizon until 2040, lays the foundations of a new organization, staffing, endowments, and training, able to fulfill its mission. This analysis was inter-departmental and inter-institutional in nature, "*at a time when security and defense challenges have taken new values"*, and the strategic planning processes now underway will influence regional security and defense, under the conditions of strengthening the military capabilities of the Russian Federation in the Black Sea region, conducting the process of strategic reflection at NATO level[45], approving a new strategy[46], and adapting the Alliance's posture[47], initiating the process of relocating US forces in Europe, all overlapping with

[43]Administrația Prezidențială*, Strategia Națională de Apărare a Ţării pentru Perioada 2020-2024 "Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări" (Presidency, The National Defence Strategy of the Country for 2020-2024. "Together for a Sure and Prosperous Romania in a World Marked by New Challenges)*, Bucharest, 2020, accessed from https://www.presidency.ro/files/userfiles/Documente/ Strategia_Nationala_de_ Aparare_a_Tarii_2020_2024.pdf, on October 06th, 2020.
[44] *Ibidem,* p. 12 (art. 50).
[45] NATO, *Secretary-General appoints group as part of NATO reflection process*, 09, June 2020, accessed from https://www.nato.int/cps/en/natohq/news_174756.htm, on 07 October, 2020.
[46] NATO, *NATO 2020: assured security; dynamic engagement*, 17 May 2010, accessed from https://www.nato.int/strategic-concept/expertsreport.pdf, on 07 October 2020.
[47] NATO, *Deterrence and Defense*, 26 May 2020, accessed from https://www.nato.int/ cps/en/natohq/topics_133127.htm, on 07th October 2020.

COVID-19 pandemic[48]. The White Paper of Defense is the main planning document of the Ministry of National Defense, which substantiates the other subsequent documents, namely the Military Strategy and the Defense Planning Directive[49].

Thus, according to the Strategy, "*the need to ensure a natural balance between national security and other vital areas, such as the economy, health or education*[50]" is highlighted. This balance has new aspects after the abusive occupation of Crimea and the pandemic generated by COVID-19, thus putting ministries and agencies in the situation to analyze and understand security but also to identify new methods of action against risks and threats. The policy of force of some undemocratic states "*which challenges the current liberal international order are the major variables that will influence the distribution of power globally and the configuration of balances of influence and regional stability"*[51]. The new revised strategy is a modern tool and connected to the realities of security in the Black Sea, requires the military to make a complex analysis of the type of forces we will have to use in the coming decades so that there are no differences between strategic approach, politico-military planning, the allocated budget of GDP and the packages of available reaction forces. This security strategy identifies that *"the absence of real multiannual budgetary planning*[52]" could have consequences that compromise research and innovation, and the development of military capabilities and commitments to NATO, the EU, and strategic partners. The long-term modernization of the Naval Forces is correlated with this strategy and can ensure a security climate in the Black Sea.

The Minister of Foreign Affairs, Bogdan Aurescu, highlighted at the informal meeting of the Council of Foreign Ministers of the member states of the Black Sea Economic Cooperation Organization (BSEC), the fact that "*the Black Sea Region will emerge stronger from the economic crisis generated by the COVID-19 pandemic only if there are common solutions and mutual trust"*[53].

In terms of the capabilities used depending on the need for maritime security and the strategies to be implemented, the Romanian Naval Forces participated in 2019 in the NATO Operation "*Sea Guardian"*, in the Mediterranean Sea, in operations and exercises with NATO permanent groups by integrating Romanian ships in five deployments, in total 97 days under the command of the NATO Allied Maritime Command, in the "Resolute Support" mission in Afghanistan, by participating for the first time a detachment of Marines, in 18 multinational

[48] CSAT, *Ședința Consiliului Suprem de Apărare a Țării (The meeting of the Country's Supreme Defense Council),* 06 October 2020, accessed from https://csat.presidency.ro/ro/comuni/sedinta-consiliului-suprem-de-aparare-a-tarii1601986459, on 07 October 2020.

[49] Monitorul Apărării şi Securităţii, Florin Jipa, *Armata are ambiţii mari: grupare de forţe întrunite de nivel corp de armată,* 06 October, 2020, accessed from https://monitorulapararii.ro/armata-are-ambitii-mari-grupare-de-forte-intrunite-de-nivel-corp-de-armata-1-33643, on 07 October 2020.

[50] Administrația Prezidențială, *Strategia Naţională de Apărare a Ţării pentru Perioada 2020-2024 "Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări" (Presidency, The National Defence Strategy of the Country for 2020-2024. "Together for a Sure and Prosperous Romania in a World Marked by New Challenges)*, Bucharest, 2020, accessed from https://www.presidency.ro/files/userfiles/Documente/ Strategia_Nationala_de_ Aparare_a_Tarii_2020_2024.pdf, on October 06th, 2020, p. 6.

[51] *Ibidem,* p. 18.

[52] *Ibidem,* p. 26.

[53] "Ministrul de Externe: *Regiunea Marii Negre va iesi intarita din aceasta criza economica doar cu solutii commune",* in Ziare.com 25 September 2020, accessed from https://ziare.com/stiri/eveniment/ministrul-de-externe-regiunea-marii-negre-va-iesi-intarita-din-aceasta-criza-economica-doar-cu-solutii-comune-1633433, on 26 September, 2020.

joint exercises, with allies and partners, outside the national territory and, last but not least, by assigning permanent positions in NATO and EU structures by the Romanian military[54].

As highlighted in the conclusions of the National Defense Strategy, its role is to continue to implement the guidelines established in 2015, and to support the institutions of the national defense system, to find answers to the evolutions of the internal and international security environment, in their efforts to ensure the safety of the citizen and the Euro-Atlantic security[55]. The new strategy corresponds to national interests, aligns to the security requirements promoted by the EU[56] resulting in the strengthening of the Eastern flank of the EU and NATO. In this regard, it is worth mentioning in the Declaration of the Brussels Summit that it is necessary to strengthen NATO's deterrence and defense posture in the Black Sea (art. 19), the development of the tailored Forward Presence (art. 26) and capacity building. operations of the Multinational Brigade and the initiation of the establishment of a land command and control capacity at corps-level (art. 30) and last but not least the NATO Ballistic Missile Defense system (art. 38) which Romania is hosting to help strengthen NATO 's defense and deterrence posture.

In the spirit of this Declaration, an increasing number of ships belonging to NATO and the US Navy have participated in maritime or joint exercises, in the Black Sea, for an increasing number of days, having positive effects in terms of security. The National Defense Strategy promotes increased participation of the Romanian Naval Forces together with those of NATO and the USA, both in operations and during the exercises, proving a major concern of the development of the culture of "*readiness*" and rapid response in crises. Future strategies must take into account the risks and limitations imposed by the pandemic and readjust to the new requirements of isolated action, with unmanned or remote-controlled equipment.

The size of the maritime force (but also of the other services) is determined and adapted to the risks and threats, depending on the objectives and Romania's interests in the Black Sea and the Danube River. The Maritime Task Group and River Task Group work continuously, together with the countries bordering the Black Sea to maintain a climate of security, strengthening diplomatic relations and mutual trust.

The allocated financial resources of 2% of GDP allow the planning of forces to operate in theaters of operations, and the multi-annual acquisition of new weapons systems or platforms. The evaluation of the necessary ships, platforms, and naval equipment was made in accordance with the strategic planning assumptions that are deduced from the NDS, and that focus on deterrence, forward presence, credibility and rapid crisis response.

---

[54] Statul Major al Forţelor Navale, *Şedinţa de autoevaluare a Forţelor Navale Române pentru anul 2019 (Naval Forces Staff, Meeting of the Naval Forces of Romania Self-Evaluation for 2019)*, accessed from https://www.defense.ro/edinta-de-autoevaluare-a-fortelor-navale-romane-pentru-anul-2019, on 07 October, 2020

[55] Administrația Prezidențială, *Strategia Naţională de Apărare a Ţării pentru Perioada 2020-2024 "Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări" (Presidency, The National Defence Strategy of the Country for 2020-2024. "Together for a Sure and Prosperous Romania in a World Marked by New Challenges)*, Bucharest, 2020, accessed from https://www.presidency.ro/files/userfiles/Documente/ Strategia_Nationala_de_ Aparare_a_Tarii_2020_2024.pdf, on October 06th, 2020, art. 212, p. 42.

[56] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy*, Brussels, 24.7.2020 accessed from https://ec.europa.eu/info/sites/info/files/ communication-eu-security-union-strategy.pdf, andConsiliul European, Brussels, 10 July 2018, *Joint Declaration on EU-NATO Cooperation By the President of the European Council, The President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, accessed from URL: https://www.consilium.europa.eu/media/36096/ nato_eu_final_eng.pdfon 22nd September, 2020.

From the point of view of the resources allocated to defense, it is difficult to fully calculate how COVID-19 affects or influences the defense budget and the level of training and readiness. Expenditure on modernization has remained the same, but a possible new epidemic wave could influence this sensitive balance by migrating funds to the fight to isolate the virus. However, the rebalancing of the budget and endowment programs is done with a bottom-up reassessment of all bodies involved in security, based on the same balance between strategies, security and forces. In this sense, is also the aspect debated in the videoconference about Romanian-American relations, organized by the think tank "*The Heritage Foundation*", where the Minister of National Defense, highlighted the dynamics of the security environment on the Black Sea, after the illegal annexation of Crimea by the Russian Federation. He highlighted that "*The endowment of the Romanian Army, .., remains a priority of my ministerial mandate*", and that "*2020 is the fourth consecutive year in which Romania provides this percentage in the budget, which makes the investments in the military equipment to continue, and training and preparedness schedules planned with the Allies and adapted to the global health crisis, to develop the military's combat capability*"[57].

Most of the programs supported as part of the modernization of the army continued to receive the established levels of funding. However, long-term modernization plans risk remaining underfunded as a result of the reallocation of funds to keep the citizen's health safety at a maximum level. At these times, when the pandemic is under some control, it is necessary to re-evaluate the strategies related to security, modernize the military capabilities to find the balance between them and to maintain Romania's interests in the Black Sea and the Danube, at the estimated level.

Conclusions

The current defense review will need to address the issues of strategy, long-term modernization, and adequate resources. More than ever, in the Black Sea region, there is an action by riparian states aimed primarily at safeguarding the interests of the citizen and sovereignty, to the detriment of maintaining regional or global security.

During the bottom-up evaluation of the strategy, a golden mean must be identified, adapted to all the requirements of the operational environment. This requires knowing the real costs, avoiding financial bottlenecks, and limiting the involvement of other bodies that could influence or divert expenditure from the initial allocation. Risks and threats to vital national interests will always produce alternatives and policy directions that prioritize decided courses of action.

We have identified two lessons regarding the approach to security in the context of maintaining the balance between security, strategy and military capabilities, in the conditions of COVID - 19, as follows:

1. Of particular importance are the side effects caused by this pandemic. The changes they bring in the fields of military, information, legislation, military, economic, research and development and last but not least security require us to periodically review the strategies and resources allocated. The potential results must be perfectly adapted to the

[57] Cătălina Băltăreţu, "Nicolae Ciucă, la dezbaterea organizată de „The Heritage Foundation" pe tema relațiilor româno-americane", in *Ziua*, 06 October, accessed from https://www.ziuaconstanta.ro/stiri/actualitate/nicolae-ciuca-la-dezbaterea-organizata-de-the-heritage-foundation-pe-tema-relatiilor-romano-americane-730551.html, on 07 October 2020.

conditions imposed by the pandemic, namely: military action with a small number of soldiers and the development of other types of military equipment that do not involve combat personnel. These results are difficult to achieve if the borders of states (or regions within them) will be closed to limit the evolution of the pandemic and, implicitly, the diminution of economic, military, and research cooperation.

2. Despite an endowment budget that may fluctuate under the given conditions, the only chance to adapt to the new conditions is to remodel and rethink all military equipment and platforms.

BIBLIOGRAPHY:

1. AAP 6, *NATO Glossary of Terms and Definitions (English and French)*, edition 2018, URL: https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600
2. Administrația Prezidențială*, Strategia Naţională de Apărare a Ţării pentru Perioada 2020-2024* Bucharest, 2020.
3. HAWSER, Anita, Defence Procurement International, *Coronavirus Strikes French Naval Vessel*, 16 April 2020, URL: https://www.defenceprocurementinternational.com/news/chemical-biological-radiological-and-nuclear/coronavirus-on-board-french-aircraft-carrier-charles-de-gaulle
4. BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap, *Security: A New Framework for Analysis*,Lynne Rienner Publishers, London, 1998, URL: https://books.google.ro/books?hl=ro&lr=&id=j4BGr-Elsp8C&oi=fnd&pg=PP9&ots=bPmaoUYs5b&sig=bGnId2N6lrJGoMYf26t6Ogu4KaM&redir_esc=y#v=onepage&q&f=false
5. BUZAN, Barry, Department of International Studies University of Warwick, 1983, *People, States and Fear: An Agenda For International Security Studies in the Post-Cold War Era*, URL: https://www.academia.edu/4780500/People_States_and_Fear_An_Agenda_For_International_Security_Studies_in_the_Post_Cold_War_Era_Barry_Buzan
6. VON CLAUSEWITZ, Carl, *Despre Război*, Editura Antet Press, 2006.
7. BĂLTĂREȚU, Cătălina, Nicolae Ciucă, la dezbaterea organizată de „The Heritage Foundation" pe tema relațiilor româno-americane, *Ziua*, 06 octombrie, URL: https://www.ziuaconstanta.ro/stiri/actualitate/nicolae-ciuca-la-dezbaterea-organizata-de-the-heritage-foundation-pe-tema-relatiilor-romano-americane-730551.html
8. Comisia Europeană, *Strategia UE privind o uniune a securității: asigurarea conexiunilor în cadrul unui nou ecosistem de securitate*, URL: https://ec.europa.eu/commission/presscorner/detail/ro/ip_20_1379, Comunicat de presă, 24 iulie 2020
9. Comisia Europeană, *Prioritate – Un nou elan pentru democrația europeană. Să ne cultivăm, protejăm și consolidăm democrația, URL:* https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy_ro
10. Consiliul European, Brussels, 10 iulie 2018, *Joint Declaration On Eu-Nato Cooperation By The President Of The European Council, The President Of The European Commission, And The Secretary General Of The North Atlantic Treaty Organization*, URL: https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf
11. CSAT, *Ședința Consiliului Suprem de Apărare a Țării,* 06 October 2020, URL: https://csat.presidency.ro/ro/comuni/sedinta-consiliului-suprem-de-aparare-a-tarii1601986459
12. BALDWIN, David A. *The concept of Security*, Review of International studies, 1997, URL: https://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf
13. BOUCHER, David, *Political Theories Of International Relations: From Thucydides to the Present*, Oxford University Press, New York, 1998.
14. Dexonline, URL: https://dexonline.ro/definitie/echilibru

15. *Dictionary of Military and Associated Terms*. S.v. "national security strategy." Retrieved October 8 2020 from URL: https://www.thefreedictionary.com/national+security+strategy and URL: https://dexonline.ro/definitie/strategie
16. TĂNASE, Tiberiu, STAN, Mircea, *Puncte de vedere privind reforma legislativă a sistemului de securitate naţională a României*, URL: https://www.mapn.ro/publicatii/2017/infosfera/ infosfera_2_2017.pdf
17. FURNISS, Edgar S. Jr., "The Contribution of Nicholas John Spykman to the Study of International Politics", *World Politics*, Vol. 4, No. 3, April 1952.
18. European Commission, *Communication from the Commission to the European Parliament, the European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions on the EU Security Union Strategy*, Brussels, URL: https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf, and Consiliul European, Brussels, 10 iulie 2018, *Joint Declaration On Eu-Nato Cooperation By The President Of The European Council, The President Of The European Commission, And The Secretary General Of The North Atlantic Treaty Organization*, URL: https://www. consilium.europa.eu/media/36096/nato_eu_final_eng.pdf
19. MACKINDER, Halford J., "*The Round World and the Winning of the Peace*", Foreign Affairs, Vol. 21, July 1943, no. 4, URL: https://people.ucsc.edu/~rlipsch/migrated/Pol177/ Round%20World.pdf
20. MACKINDER, Halford J., *Democratic Ideals and Reality. A Study in the Politics of the Reconstruction by the Right Honorable Sir Halford J. Mackinder*, National Defence University Press, Washington, 1942.
21. WALTZ, K.N., *Theory of International Politics,* S. I. Columbia University, Ed. Long Grove, Waveland Press, Boston, 1979.
22. TRITLE, L.A., *Thucydides and the Cold War, în M. Meckler* (ed.), *Classical Antiquity and the Politics of America: From George Washington to George W. Bush*, Waco, 2006.
23. LARSON, Eric V., ORLETSKY, David T. and LEUSCHNER, Kristin J., Balancing *Strategy, Forces, and Resources: Lessons for the Current Defense* Review. Santa Monica, CA: RAND Corporation, 2001, URL: https://www.rand.org/pubs/research_briefs/RB73.html
24. LAYNE Christopher, *"The Unipolar Illusion: Why New Great Powers Will Rise"*, International Security, Vol. 17, No. 4, Spring 1993.
25. *Legea nr. 51/1991 privind securitatea naţională a României*, republicată în 2014, URL: http://www.dreptonline.ro/legislatie/legea_51_1991_securitatea_nationala_romaniei_republicata .php
26. RUF, Frederick J., *William James and the Stylistic Making of a Disorderly World. The Creation of Chaos*, State Univerity of New York Press, Albany, 1991, URL: https://books.google.ro/ books?id=8xZdZCs3d-YC&pg=PA4&dq=who+was+Louis+J.+Halle&hl=ro&sa=X&ved=0ah UKEwjWpqSR0Oj WAhVGBsAKHSExD_ oQ6AEIWDAH
27. ANTONIU , Bogdan, DINU, Mihai-Rudolf, Ministerul Educaţiei şi Cercetării, *Istoria relaţiilor internaţionale în secolele XIX – XX*, 2005, URL: http://hiphi.ubbcluj.ro/studii/Public/File/ cursuri/suporturi_conversie/Relatii-internationale.pdf
28. JIPA, Florin, Monitorul Apărării şi Securităţii, *Armata are ambiţii mari: grupare de forţe întrunite de nivel corp de armată*, 06 October 2020, URL: https://monitorulapararii.ro/armata-are-ambitii-mari-grupare-de-forte-intrunite-de-nivel-corp-de-armata-1-33643
29. NATO, *Deterrence and defence*, 26 May. 2020, URL: https://www.nato.int/cps/ en/natohq/topics_133127.htm
30. NATO, *NATO 2020: assured security; dynamic engagement*, 17 May 2010, URL: https://www.nato.int/strategic-concept/expertsreport.pdf
31. NATO, *Secretary General appoints group as part of NATO reflection process*, 09, iunie 2020, URL: https://www.nato.int/cps/en/natohq/news_174756.htm
32. SPYKMAN, Nicholas J., *America's Strategy in World Politics: The United States and the Balance of Power*.
33. BATEMAN, Sam, *Safety of life at sea: Covid-19 and naval operations*, The interpreter, 20 aprilie 2020, URL: https://www.lowyinstitute.org/the-interpreter/safety-life-sea-covid-19-and-naval-operations

34. LA GRONE, Sam, Carrier Theodore Roosevelt COVID-19 Outbreak Investigation Complete, CNO Now Reviewing Report, USNI News, URL: https://news.usni.org/2020/05/27/carrier-theodore-roosevelt-covid-19-outbreak-investigation-complete-cno-now-reviewing
35. Statul Major al Forţelor Navale, *Şedinţa de autoevaluare a Forţelor Navale Române pentru anul 2019*, URL: https://www.defense.ro/edinta-de-autoevaluare-a-fortelor-navale-romane-pentru-anul-2019
36. GHERVAS, Stella, *Congresul de la Viena şi pacea europeană*, Historia, URL: https://www.historia.ro/sectiune/general/articol/congresul-de-la-viena-si-pacea-europeana
37. THUCYDIDES, *The landmark Thucydides, a comprehensive guide to the peloponesian war*, Ed. R. B. Strassler, New York, Touchstone, Rockefeller Centre, 1998.
38. TĂNASE, Tiberiu, STAN, Mircea, *Puncte de vedere privind reforma legislativă a sistemului de securitate naţională a României*, URL: https://www.mapn.ro/publicatii/2017/infosfera/infosfera_2_2017.pdf
39. DUNNE, Tim, SCHMIDT, Brian C., *Realism*, URL: http://www.academia.edu
40. VAVASSEUR, Xavier, Naval News, *Theodore Roosevelt, Nimitz Carrier Strike Groups Operate Together In Philippine Sea*, 23 June 2020, URL: https://www.navalnews.com/naval-news/2020/06/theodore-roosevelt-nimitz-carrier-strike-groups-operate-together-in-philippine-sea/
41. VAVASSEUR, Xavier, USNI News, *French Carrier Strike Group Begins 'Foch' Deployment*, January 23, 2020, URL: https://news.usni.org/2020/01/23/french-carrier-strike-group-begins-foch-deployment, on 09 October 2020.
42. ZAIM, Diana, September 4th, 2020, Calea Europeană, Ludovic Orban, discurs la "Black Sea and Balkans Security Forum": Puterea economică a UE, adevărata forță de atracție a proiectului European", URL: https://www.caleaeuropeana.ro/ludovic-orban-discurs-la-black-sea-and-balkans-security-forum-puterea-economica-a-ue-adevarata-forta-de-atractie-a-proiectului-european/
43. Ziare. Com, Ministrul de Externe: *Regiunea Marii Negre va iesi intarita din aceasta criza economica doar cu solutii comune*, Vineri, 25 September 2020, URL: https://ziare.com/stiri/eveniment/ministrul-de-externe-regiunea-marii-negre-va-iesi-intarita-din-aceasta-criza-economica-doar-cu-solutii-comune-1633433

EURASIA – THE GEOPOLITICAL AND GEOSTRATEGIC BET OF THE 21st CENTURY

Silviu NEGUȚ, Ph.D.
Professor, Geographer and Geopolitical Analyst, University of Economic Studies, Bucharest, Romania. Email: silviu.negut@gmail.com

Abstract*: Eurasia, the super continental mass that holds the largest share in the world`s size, population and economic power, has become the main region of interest on the planet. Within it, several geopolitical –geostrategic areas/regions have been mainly configured with great relevance (each with its actors/players –including some from outside this area – and with its problems/interests), such as North-East Asia, Central Asia, South-East Asia, Middle East, the Indian Ocean, Western Pacific, South China Sea, East China Sea, the Black Sea, the Arctic Ocean, etc. The first two decades of the 21st century, in addition to the spectacular economic assertion of some particular Asian countries, have increased the dynamism and complexity of the security environment around the world, largely due to some events that previously occurred in Eurasia: The Georgia war (2008), Russia`s takeover of Crimea (2014), US President Donald Trump`s unsuccessful attempts to ease relations with North Korea, China and Russia, tensions in the Middle East, the contradictory effects of the "greatest geo-economics project of the 21st century" – the New Silk Road), etc. Here, too, the game takes place between the two great present and future powers, the United States and China, and this game depends, or at least is influenced by other Eurasian actors.*

Keywords*: Eurasia; Eurasianism; geopolitical – geostrategic areas/ regions; game-players; superpowers; powder keg/cauldron; One Belt, One Road.*

1. General considerations

Eurasia, the super continental mass that holds the largest share in the size, population and economic power of the world, has become the main region of interest on the planet. Within it, several geopolitical-geostrategic areas/regions have been set up with great relevance worldwide (each with its actors/players – including some from outside – and with its problems/ interests), such as: North- East Asia, Southeast Asia, Central Asia, the Middle East, the Indian Ocean, the Western Pacific, the South China Sea, East China Sea, the Caspian Sea and the Caucasus, the Black Sea, the Balkans, etc.

During the first two decades of the 21st century, in addition to the spectacular economic assertion of some (especially Asian) states, the dynamism and complexity of the global security environment have increased, largely due to events in Eurasia: the war of Georgia (2008), Russia's takeover of Crimea (2014), President Donald Trump's failed attempts to de-escalate relations with North Korea, China and Russia, the tensions in the Middle East, with a possible conflict between Iran and Saudi Arabia (the leaders of the two main Islamic currents, each with its own acolytes), the contradictory effects of "the greatest geo-economics project of the 21st century – the New Silk Road, etc. Here, too, the game takes place between the two great powers of the present and of the future, at least of the near future, the United States (which wants to retain its rank of superpower, as it has lost the hegemon, we believe) and China (having as objective its metamorphosis from great power to superpower).

This game depends on, or at least is influenced by other Eurasian actors, such as Russia, Japan, India, South Korea, North Korea, Iran, Saudi Arabia, and to a lesser extent, Germany, France, the United Kingdom, and so on.

In this study I have used the terminology of political-geostrategic regions (and not only geopolitical regions or geostrategic regions) because, if we carefully analyze the mentioned/identified above regions/zones, we may find the following:

a) on one hand, some areas have been differentiated which, due to their geographical position and the association of some factors that impose a certain physiognomy and territorial homogeneity and/or riches, have aroused the interest of some external powers;

b) on the other hand, both the countries in the respective region and those that targeted them have developed protection/defense strategies and, respectively, occupation or subordination in one form or another.

As a result, such regions are ambivalent, being both geopolitical and geostrategic.

2. Name, geographical position, dimensions

Eurasia is the continental ensemble or supercontinent formed by Europe and Asia (hence the name), which, with the 57.25 million km^2[1] (of which 2.75 million km^2 adjacent islands), owns more than a third (37%) from the extent of the planet's land and concentrates almost ¾ of the planet's population. Continental Eurasia is located exclusively in the Northern hemisphere of the planet, only some islands and archipelagos (Indonesian Archipelago) being South of the Equator, so in the Southern hemisphere. It is also found in the vast majority in the Eastern hemisphere, with only a small European segment in the Western hemisphere (west of the "0"/Greenwich Meridian). It measures 16,000 km from West to East (of which 10,000 km in Asia, the rest in Europe) and 7,800 km from North to South (in Asia, in Europe only 4,800 km). It is also the only land mass on the planet watered by the waters of all four oceans (Atlantic, Pacific, Indian and Arctic); from 1869, with the commissioning of the Suez Canal, the only connection with another continent was broken, namely Africa (the connection was made through the Suez Isthmus).

The creator of the Eurasia name is the Austrian geologist Eduard Suess (1831-1914), who noticed that Europe is nothing more than a slightly larger peninsula of Asia. It was not long after it gained a geopolitical meaning, thanks to the British Halford Mackinder, in the famous 1904 study *"The Geopolitical Pivot of History"*, in which he launched the theory of the heartland. The same geopolitical meaning is found in the famous "1984" novel (published in 1948) by the English visionary writer George Orwell (1903-1950), *Eurasia* being one of the three super states vying for supremacy in the world.

Eurasia, with the highest average altitude in Asia (almost 1000 m) and lower in Europe (about 300 m), is the continental mass that encompasses absolutely all categories of major landforms. The climate is extremely varied, being practically present all types of climate on the globe, from the equatorial to the polar. In terms of hydrography, it is a region of great contrasts: areas with a high density of the hydrographic network (rivers carry their waters to all four oceans), but also large endorheic areas (unrelated to the Planetary Ocean). In turn, the vegetation and fauna are varied and rich.

[1] A.N.: The main statistical sources used for this study are: Horia C. Matei, Silviu Neguț, Ion Nicolae (2020*), Enciclopedia Statelor Lumii*, Ediția a 16-a, Ed.Meronia, București; *Britannica:Book of the Year 2019; CIA. The World Factbook 2020:* https://www.cia.gov/library/publications/resources/the-world-factbook/index.html*; United Nation Statistical Yearbook 2019:* https://unstats.un.org/unsd/publication/statistical-yearbook/files/syb62/syb62/.pdf; *Calendario Atlante de Agostini 2020,* Instituto Geografico de Agostini*; SIPRI Yearbook 2019*: Armaments, Disarmament and International Peace Research Institute:www.sipri.org/databases.

At the same time, Eurasia has varied and rich natural resources, holding world supremacy in several areas: arable land with permanent crops, forest fund, irrigated land, the economical hydropower potential, fossil mineral fuels (peat, coal, oil, natural gas), ores; ferrous and non-ferrous (tin, nickel, vanadium, manganese), non-metallic substances (mercury, salts of potassium and salt , sulfur, magnesite and fluorine), as well as lanthanides – or rare earths, used in the construction of lasers – almost all world reserves.

3. The concept of Eurasia

3.1. Eurasia in the Western conception

In order to understand Eurasia, implicitly its geopolitical and geostrategic position, we must first turn to two established theories: *the heartland* (the British Halford Mackinder) and *the rimland* (the Dutch-American Nycholas John Spykman), plus a number of more recent interpretations, including those of the Russian Aleksandr Dughin and the American Robert D. Kaplan. Paradoxically, two of the best and most famous analysts in the field, the French Yves Lacoste (coordinator of the giant "Dictionnaire de géopolitique")[2] and Hervé Coutau-Bégarie (in turn the author of the huge "Traité de stratégie")[3] they totally neglects it.

We must especially remember the theory of the stepped *heartland*, formulated by Mackinder[4]:

Who rules East Europe commands the Heartland
Who rules the Heartland commands the World Island
Who rules the World Island commands the World.

Basically, according to Mackinder, the *Heartland* is Eurasia, and *World Island* – the Old World, respectively Eurasia plus Africa.

The other theory without which the concept of Eurasia, that of the *rimland*, cannot be fully understood, does not focus on the continental *heartland*, constituting an intermediate area between it and the peripheral seas. Therefore, the "pivot" is no longer Russia, as in Mackinder's theory, but the *rimland*, the "ring" around it. Spykman practically modifies Mackinder's formula by stating: "Whoever dominates Eurasia, holds in his hands the destinies of the world"[5].

3.2. Eurasia in the Russian conception

Russian analysts who leaned on this concept, *Eurasia* and *Eurasianism* (using the variant *Eurasiatism*) – and did so in two distinct and distant phases in time: the first, after the Bolshevik Revolution and the establishment of the Soviet Union, starring Pyotr Nikolaevich Savitsky (1885 - 1968), the second, after the collapse of the Soviet Union, with the spearhead Aleksandr Dughin (b. 1962).

Savitsky stated: "Russia – Eurasia is the center of the Old World. Extend this center and all its other parts, and the whole system of these continental peripheries (Europe, Inner Asia, Iran, India, Indochina, China, Japan) would turn into a "scattered construction". And he

[2] Yves Lacoste (sous la direction de ~; 1995), *Dictionnaire de géopolitique,* Flammarion, Paris.
[3] Hervé Coutau-Bégarie (2008), *Traité de stratégie,* VI-a, Ed. Economica, Paris.
[4] Mackinder made these statements not in the 1904 article The Geographical Pivot of History, as it is usually written (then he only launched the idea of the triptych Heart Island- World Island- World), but in his study published 15 years later: *Democratic Ideals and Reality. A Study in the Politics of Reconstruction*, Henry Holt & Co, New York, p. XVIII.
[5] Nicholas John Spykman (1942), *America's Strategy in World Politics. The United States and the Balance of Power*, Harcourt, New York.

goes on to say: "Russia is neither Asia nor Europe, it is a separate geopolitical world" and that "Eurasia has played a unifying role in the Old World."

In turn, Aleksandr Dughin revives over time, in the Russian spirit, the concepts of *Eurasia* and *Eurasianism (Eurasiatism).* A follower of the "law of the dualism of the elements" (*Land against the Sea*), respectively the opposition between t*ellurocracy* (land-based hegemony) and *thalassocracy* (sea power), Dughin introduces into the equation Eurasia and, obviously, Russia, with all the related pro-Russian issues: Russia's geopolitical predestination, today's Russia (Russian Federation) does not represent the all-Russian State, Russia – "the third Rome" (after Rome and Constantinople), the Russians – "the messianic people", etc. As a result, he speaks of the need to "coagulate the Empire," to unify the Eurasian territories under Russian protection as the "axis of history." Moreover, according to Dughin, "the imperative of Russia's geopolitical and geostrategic sovereignty consists not only in resuming alliance relations with Eastern European countries, but also in including in the new Eurasian strategic bloc the continental Western states (primarily the Franco-German block, which tends – according to the analyst – to free itself from the tutelage of NATO pro American and the continental Eastern states (Iran, India, Japan)"[6].

The same Dughin argues, no more, no less, that the lack of "living space" and economic necessities has forced the Russian people to expand their borders in all directions: "The lack of land has never been the real cause of the construction of the Russian Empire. The Russians were expanding as *bearers of a special mission*, whose geopolitical design consisted of a deep awareness of the need to unite giant territories of the Eurasian continent.[7] And he apotheotically concludes that: a *New Eurasian Empire* must be built and that *"The New Eurasian Empire* (emphasis added) is inscribed in the geographical and historical predestination of world history (...). The interests of the Russian people are inextricably linked to the establishment of such a continental structure."[8].

4. Geostrategic players and other players on the Eurasian stage

There are many "players", in the geopolitical and geostrategic sense of the term, in Eurasia, maybe even too many, which could be grouped into: proper geostrategic players, geostrategic players into question and pivotal countries.

A. Proper Geostrategic players, respectively the most important, with great influence, such as China, Russia, India, Indonesia, Germany, France and others, belonging to the continental mass itself, and especially the United States of America, outside it.

- **China**

It is already considered to be the main geostrategic player in Eurasia. In fact, even a hundred years ago, the British geopolitician Halford Mackinder was a prophet regarding China, considering it the largest continental nation in Eurasia. China has advantages: an area (9.6 million km^2) as much as the United States and, respectively, Europe, a population (1.4 billion inhabitants) that represents almost 1/5 of the planet's population and with a GDP that places it even on the first place at *ppc* and on the second with nominal GDP (after the USA), at the same time a nuclear, cosmic and military power (the second as investments in the field, after the USA and at a great distance from Russia). He is also a permanent member of the UN Security Council. In addition, in 2017, it launched the largest economic project of the 21st century in the world – already called the "third millennium project" – which has strong

[6] Aleksandr Dughin (2011), *Bazele geopoliticii și viitorul geopolitic al Rusiei,* Editura Eurasiatica, București, p. 116.
[7] *Idem*, p. 130.
[8] *Idem*, p. 145.

geopolitical and geostrategic connotations: *the New Silk Road.* Communist China also knows how to combine *hard power* with *soft power.*

- **Russia**

Certainly, the Soviet Union was the most important Eurasian geostrategic player in the second half of the century XX, - and, at the same time, one of the two great players in the world. But, for the Russian Federation the same position is questioned, which considers itself (and is recognized) as the heir of the Soviet colossus, although it still has a huge area (17.01 million km^2, the largest state) and a significant population (142 million inhabitants, 1st in Europe, 6th in Eurasia and 9th in the world) and relevant economic power (7th as GDP ppc and 11th in nominal GDP), plus other strengths: it is an atomic and cosmic power (in both cases the second largest in the world, after the USA), a great military power (although lately the budget in this field is at a great distance from that of the United States and China). It is more than obvious that Russia wants, aims, to be the main geostrategic player in the world and, at least Eurasian at the present moment, only that it has formidable competitors in both cases.

- **India**

This state has become the most interesting geopolitical/geostrategic player on the Eurasian and world scene, thanks to its recent evolution that has made it, despite the great contrasts, a possible real great power. First, it has a considerable area (3.29 million km2) and a huge population (1.33 billion inhabitants, 2019), ranking 2nd in the world, after China, which, according to most forecasts, will surpass it not long after (2025-2030). Or, as it is known, the demographic potential will become more and more relevant in the future or, as the American analyst Fareed Zakaria says, "if demography means destiny, the future of India is assured"[9].Another important asset of India is the economic power, which rises dramatically in the world hierarchy, with a GDP that has grown from only 358 billion $ (1996, 14th place in the world) at 7,410 billion $ (2019, 3rd place in the world, after China and USA). In recognition of its emerging economic power, India has become a member of the BRICS – the group of the strongest "emerging economies" – and the G20. India is also becoming a military power, possessing the nuclear weapon and focusing more and more on the cosmic side (in October 2008 it launched a spacecraft to the Moon, Chandrayan 1). Also in this spirit, it is worth mentioning that, lately, India has become the largest arms importer, spending $ 15.6 billion between 2008 and 2012, twice as much as the second-ranked China.

- **Germany and France**

Both can beconsidered geostrategic players in Eurasia - as well as on the entire planet, by the way – due to the position and power they have within the significant regional bloc, the European Union (<Framania>>) – France and thanks to its role as a significant colonial power in Asia, where it still has influence. France is larger and Germany more populated. Both have strong savings, with a nominal GDP of 3,863 billion $ Germany (3rd place in Eurasia and 4th in the world) and 2,707 billion $ France (6th place in Eurasia and 7th in the world).

France or the Hexagon seems to have a few more advantages, thanks to the perfect geostrategic construction, and the second marine empire in the world (about 14 million km^2, being surpassed only by the USA), plus the quality of permanent member of the Security Council of The UN, as military power (including the atomic weapon and one of the most powerful deterrents in the world) and diplomatic power, with long traditions in the field.

Germany, in turn, has assets that qualify it as a geostrategic player in Eurasia (and also in the world): a great economic power (although it has recently lost its 3rd place in the world, which it held for a long time, and, more importantly, for a long time the world's largest

[9] Fareed Zakaria (2009), *Lumea postamericană*, Editura Polirom, Iași, p. 127.

exporter, now the second, has again become a major military power, allocating 1.5% of GDP annually, which places it in 7th place in the world, with about 50 billion $.

- **United States of America**

The United States is the only geostrategic player outside Eurasia. In fact, the United States was the first power to notice the geopolitical and geostrategic stake of Eurasia, even before the dissolution of the Soviet Union, thanks to the existence of the two great communist powers in its heart (USSR and PRC), which is why it supported the construction of the European Economic Area (now the European Union) and the military bloc (NATO) and also supported both economically and militarily a number of states in eastern Eurasia, first Japan and South Korea.

Huge country (9.83 million km^2, 3rd place in the world), as the whole European continent, and well populated (333 million inhabitants, the same place in the world), has an enviable geostrategic position: in the middle of the North American continental mass, with wide access to the two great oceans of the planet (Pacific and Atlantic) and with peaceful neighbors (Canada to the north, Mexico to the south), with an advanced pawn in the Arctic (Alaska) and another in the heart of the Pacific (Hawaii). A country with huge natural resources, both soil and subsoil, but which still remains dependent on imports of raw materials.

Following the terrorist attacks of September 11, 2001, which dispelled the myth of the invulnerability of the "American fortress," the United States adopted a new foreign policy doctrine, establishing that it was entitled to use military force in preventive strikes against any state that supports terrorist movements or intends to produce weapons of mass destruction, respectively the theory of *preventive war*. As a result of such acts, the theory of *global leadership* emerged or, as analyst Zbigniew Brzezinski says: "The self-coronation of the American president as a global leader was a moment of historical time (...). The American president has simply begun to behave as a global leader without any official international blessing."[10]

Today, at the beginning of the third millennium, the United States remains the world's great power, especially economic (nominal GDP) and military, and continues to believe in the founding myths of American society and the leading role of providence. However, they have to face a series of actors/players, competitors, absolutely all from Eurasia: the European Union, whose construction it has supported for a while, China, which competes in full, especially in the Asia-Pacific area, and not last, Russia, which remains the second largest nuclear power on the planet and one of the world's major energy forces. However, as the two French analysts appreciate, "no nation in the world can ignore the existence and influence of the United States. Directly or not, the world has entered a gravitational system around the United States".[11]

B. Unsettled Geostrategic players (Players under question) are the states that according to many analysts currently lack some assets to be fully considered leading actors in Eurasia: Great Britain, Japan, Indonesia.

- **Great Britain**

It is obviously a great power, except the surface, having many Strengths: a relatively large population (65.8 million inhabitants, among the top 15 in Eurasia), a large economic power (5th place in Eurasia and 7th in the world in nominal GDP), a significant military power (holds the atomic weapon and has a strong and competitive military fleet), is a

[10] *Zbigniew* Brzezinski, *A doua șansă. Trei președinți și criza superputerii americane,* Editura Antet XX Press, Filipeștii de Târg, p. 5.
[11] Aymeric Chauprade, François Thual (2004), *Dicționar de geopolitică: state, concepte, autori*, Editura Corint, București, p. 318.

permanent member of the UN Security Council, etc. However, although much of its colonial empire was in Asia and still has some influence in the area thanks to the Commonwealth, according to some analysts, it can no longer be considered a geostrategic player, as it manifests itself mainly in the wake of the United States.

- **Japan**

Although, like the United Kingdom and Germany, it does not benefit of a large surface, it has other advantages: an exceptional economic power, long ranking 2nd in the world (now 3rd in nominal GDP and 4th in ppc GDP) and a growing and modern military power - the military budget is around 50 billion $ annually (8th place in the world). However, Japan is also not considered a geostrategic player in Eurasia, mainly for two reasons: the first – its sphere of influence is blocked by China and the Korean Peninsula, the second – is that the Japanese state prefers to still stay under the "military umbrella of the United States."

- **Indonesia**

It is one of the largest (1.9 million km^2, 6th place in Eurasia and 14th on globe) and populated countries (265 million inhabitants, 3rd place in Eurasia and 4th in the world), rich in natural resources (land, forestry, minerals - coal, oil and natural gas, nickel, tin, etc.), and has recently added, thanks to a sustained growth, a significant economic power (6th place in Eurasia and 7th in the world to GDP ppc). It has other advantages, including: it is the most populous Muslim country (90% of the total population, which means over 230 million people) and controls the largest navigable system of straits in the world.

C. Pivot countries, which, through their geopolitical and geostrategic position and some strengths, can influence the Eurasian games, joining some of the aforementioned geostrategic players or trying, on their own, to obtain a certain position and sphere of influence that propel them to a more favorable position: Iran, Saudi Arabia, South Korea, Turkey, Ukraine (questioned after the events of 2014) and, paradoxically, Azerbaijan.

- **Turkey**

With a considerable area (almost 800,000 km^2) and a significant population (82 million inhabitants, 11th place in Eurasia and 18th in the world), Turkey enjoys an exceptional geostrategic position: on two continents, exit to four seas and located on the axis of great economic, geopolitical and geostrategic importance, linking Western and Central Eastern Europe with Middle East. The spectacular economic growth of recent times is added to the military budget, which is approaching 30 billion $ annually, which means 2.3% of GDP. Somehow became an enemy of the European Union (because for some reason it drags its acceptance as a member) and of the United States (also for several reasons, including the fact that it did not extradite the scholar and preacher Fethullah Gülen, the number 1 enemy of President Erdogan), Turkey has come very close, especially to Russia: although a NATO member, it has bought Russian military equipment that does not comply with Alliance rules (including S 400 missiles).

- **South Korea**

Although small (only about 100,000 km^2) and with a population of 52 mil., which does not numerically compete even with some regional powers, South Korea qualifies as a pivotal country due to its geographical and geostrategic position, respectively in the Korean Peninsula, one of the most sensitive areas of the planet (with possible consequences on a very large scale). However, its position as a "pivotal country" is also due to its great economic power (9th place in Eurasia and 12th place in the world, respectively, as nominal GDP) and its great capacity to penetrate foreign markets and, last but not least, its important military budget, which reached 34 md. $ annually, respectively 2.8% of GDP (one of the highest values for a developed country), as well as the partnership with the United States.

- **Iran**

A very large country (1.65 million km2) and well-populated (85 million inhabitants), Iran is very rich in mineral resources, especially hydrocarbons, with significant reserves and production of both oil and natural gas, thanks mainly to them having a significant GDP (14th place in Eurasia and 18th in the world in GDP ppc). The leader of Islamic Shiism has distanced himself from the United States and the European Union, linked primarily to the uranium enrichment process, the pre-nuclear phase and, in turn, the rapprochement of powers such as Russia and China in the first place, but also with some problem states, like Syria and Venezuela.

- **Saudi Arabia**

Larger country than Iran (2.15 million km2 - 5th place in Europe and 12th globally), but less populated (34.2 million inhabitants) and with a similar economic power (even a little stronger), also based on hydrocarbons, is generally included in the category of pivotal countries. This, like its Shiite enemy (Iran), wants a great power, but, although it occupies most of the Arabian Peninsula with an exceptional geostrategic positioning, it is practically bounded by no less than six states (Yemen, United Arab Emirates, Qatar, Bahrain, Kuwait, Iraq), which does not allow it to have a sphere of influence.

Some analysts include between the pivotal countries also *Ukraine and Azerbaijan*. However, Ukraine has serious problems, being on the verge of dismemberment on geopolitical, religious (Orthodox - Catholic) and economic (gap between the various regions) criteria. It has already lost Crimea (in 2014), and Donetsk and Lugansk, with the same support of Russia, proclaimed themselves people's republics and organized their own administrative apparatus. In contrast, Azerbaijan, although a small state (less than 100,000 km2 and only 10 million inhabitants), has an extraordinary geostrategic position, which allows it to connect the Caspian region (rich in hydrocarbons) with consumers, thus being included in all projects in the field, respectively alternative routes for hydrocarbons in the Caspian Sea region and Central Asia.

5. Regions of great interest and tensions

5.1. The Korean Peninsula

Following the "Korean War", concluded by the Panmunjon armistice signed on July 27, 1953, the peninsula was divided into two states: the Democratic People's Republic of Korea/North Korea (120,538 km2 and 25.6 million inhabitants, 2019) and the Republic of Korea / South Korea (99,720 km2 and 51.8 million inhabitants, 2019), totally different as a political system (first, communist – with the first "communist dynasty in the world" –, second, democracy) and economic (first, planned economy, second, market economy).

The *process of reunification* of Korea, which has been talked about since the separation, is far from complete, due to the large gaps between the two countries, which are getting worse day by day, plus the possession of nuclear weapons by communist Korea. During the reign of Kim Jong Il (the second president of the dynasty), he proclaimed himself a nuclear power (February 2005) and experienced a ballistic missile (July 5, 2006), followed by an underground nuclear explosion (October 9, 2006). Despite international protests, UN Security Council sanctions and resolutions (last in 2013), Communist Korea continued to conduct new missile tests and a new underground nuclear explosion. The third representative of the "Kim Communist Dynasty", Kim Jong Un, who became president in December 2011, continued his father's nuclear policy, even succeeding in successfully testing a hydrogen bomb (January 6, 2016).

The Korean Peninsula is part of Northeast Asia, one of the several major geopolitical and geostrategic regions of Eurasia with special significance in international politics, where the opposing interests of two alliances meet: a continental (*telurocratic*), consisting of Russia, China and North Korea (all three holders of the nuclear weapon), and another oceanic (*thalassocratic*), consisting of Japan, South Korea, and the United States (only the latter possessing the nuclear weapon).

As it is hard to believe that the North Korean dictator will voluntarily give up the nuclear weapon (this being his only asset), the solution of the Korean Peninsula problem falls into the following possible scenarios for the future order in Northeast Asia: a particular country will play the leading role (*Pax Americana, Pax Sinica, Pax Nipponica or Pax Korean*), an order with several players *(bigemony, trigemony, bipolarity, multipolarity*) and *Pax Consortis* - mutual cooperation between the powers of Northeast Asia and, respectively , Russia and the United States.

Apparently a local conflict, in reality it is one that concerns the whole of Eurasia and even the entire planet, as the use of nuclear weapons in an open conflict would have consequences on a global scale.

5.2. The Middle East

The Middle East is the geographical area around the Persian Gulf, including the Arabian Peninsula (with six states: Saudi Arabia, Kuwait, Bahrain, Qatar, the United Arab Emirates and Yemen), plus Iran and Iraq. The place where the continents, cultures and major religions of the world meet, is the most fragile segment of the world geopolitical system. The Middle East is a fully Islamic region, but split due to the two main currents: Sunnism (about 90% of the total, led by Saudi Arabia) and Shiism (about 10%, led by Iran), the two states, today regional powers, being in open conflict.

The main asset of the region is hydrocarbons, holding almost half of the world's oil reserves and over 40% of natural gas. It includes some of the world's largest producers in the field (5 of the top 10 world oil producers and 3 of the top 10 natural gas producers). As a result, the interest for this region of deficient powers in the field, usually large powers, is justified. In the same way, we understand why, in recent decades, most of the armed conflicts have focused on oil - "oil-scented wars" - such as the Iraqi - Iran war, the Iraqi - Kuwaiti war ("Second Gulf War"), as well as US intervention in Iraq (2003) - the famous "preemptive war".

At the present moment, the geopolitical situation in the Middle East region is very complicated – not infrequently with explosive accents – not only because the internal fragmentation having as spearheads two strong actors (Iran and Saudi Arabia), but also added the games of the great powers, which have their own interests, especially the United States, Russia and China.

5.3 "Europe's powder keg" and "Asia's powder keg"

"Europe's powder keg" was a phrase applied to the Balkans in the 19th century, as there were many conflicts here as the Ottoman Empire became "sick of Europe" and the nation's struggle for emancipation under "Ottoman rule". In addition, the European powers, especially Russia, the Austro-Hungarian Empire, Great Britain and Germany, which sought to take the place of the Ottoman Empire, expressed interest in the Balkan region.

The Balkan wars have sharpened international contradictions, contributing to the outbreak of World War I. In fact, the spark of the great conflagration ignited here, with the assassination of Archduke Franz Ferdinand, heir to the Austro-Hungarian throne, in Sarajevo (June 28, 1914), as a pretext for the Triple Entente to unleash war on Serbia (a month later) and through the system of alliances, of world war.

The Balkans will regain its sad reputation (as a "powder keg") at the end of the twentieth century, when the break-up of Yugoslavia takes place, due to the accentuation of centrifugal tendencies amid the exacerbation of nationalisms, eventually the federation dissolving completely – even more, a province become secessionist will proclaim its independence (Kosovo). It is worth mentioning that in Croatia and Bosnia and Herzegovina, the war broke out with unprecedented violence and cruelty in post-war Europe. And things will probably not stop there, as Bosnia and Herzegovina remains a small "powder keg" ("cauldron") as the three ethnic groups (Serbs, Croats and Bosnians) continue to operate with their own political, economic and social structures.

The phrase *"the powder keg of Asia"/"Asia's Cauldron"* for the South China Sea was first used by American geopolitician Robert D. Kaplan in the book with this title, and as a subtitle "*the South China Sea and the End of a Stable Pacific*".[12] This huge sea (3.48 million km^2 – almost 9 times wider than the Black Sea) belongs to the Pacific Ocean and connects, mainly, between the maritime world of the Middle East and the Indian subcontinent and that of Northeast Asia. It is bordered by 10 countries and a territory (Taiwan), of which five countries (PR of China, Vietnam, Malaysia, Brunei and the Philippines) and the mentioned territory are involved in the phenomenon that turned this marine stretch into a "powder keg", a cauldron as Kaplan is calling it. If we add the involvement of the United States as a global power, things get very complicated.

The apple of discord is some seemingly insignificant droughts, consisting of about 250 islands (the largest, Itu Aba has only 36 hectares!), atolls and coral reefs (usually below sea level), grouped in the islands of Paracel (Hsisha), Spratly (Nanshan), Pratas (Dongsha) and Scarborough Reef. The main stake is not mainly the rich reserves of hydrocarbons (estimated by Kaplan to be 7 billion barrels and 900 billion cubic meters of natural gas), but especially the control over the great maritime route mentioned before and, especially, the expansion of the strategic hinterland of China with no less than 1000 nautical miles (over 1850 km).

If for a long time China was reduced to being a significant land power, for some time it has added *its strategic project of the sea*, namely the introduction under the jurisdiction of the Chinese state of large marine spaces. Things got complicated after that between December 2013 and October 2015, China built seven artificial islands (meaning 300 acres) over the reefs of the Spratly Islands (by storing gravel and sand), islands that house buildings, ports and even airstrips, the latter arousing suspicion that the Chinese state is arranging a military facility, thanks to which it could control the maritime and air traffic in the South China Sea. In fact, as Paul Dobrescu points out, China's message is very clear; "The South China Sea enters under the Chinese sphere of influence".[13]

Although, in practice, the issue is essentially legal in nature, China refuses arbitration by the Hague International Court of Justice. President Xi Jingping made this very clear in an interview with Reuters on October 17, 2015: "The islands and reefs of the South China Sea are Chinese territories inherited from our ancestors. The Chinese people will not allow anyone to violate China's sovereignty over its rights and interests in the South China Sea. "

In fact, here the fight is between China and the United States, the latter striving to maintain its influence of global power in this fragile area of geopolitical junction.

In a similar situation is *the East China Sea* (1.2 million km^2), located north of the South China Sea, where there is a tripartite dispute between China, Japan and Taiwan for the island of Diaoyu/Senkaku/Tiaoyutai. The stakes are the same as for the patches of land in the South China Sea: the oil fields, the location on the aforementioned important sea route and, last but not least, the expansion of the Chinese hinterland.

[12] Robert D.Kaplan (2014), *Asia's Cauldron. The South China Sea and the End of a Stable Pacific*, 2014.
[13] Paul Dobrescu (2016), *Crizele de dupa criză. O lume fără busolă și fără hegemon*, Ed.Litera, Bucuresti, p.333.

5.4. The Caspic Sea

Located at the crossroads between Europe and Asia, over time the Caspian Sea area has given Europeans access to the legendary riches of the Orient, while the Orientals (mainly traders) have opened their doors to European markets (the most conclusive example being *the Road Silk*), practically through the Mediterranean Sea, where three worlds met and still meet: Asian, European and African.

The Caspian Sea is one of the oldest and most important oil regions in the world. Lately, it has returned to attention, mainly due to hydrocarbons, first oil, and then natural gas. The interest is so great that it has been reflected even in the estimation of oil reserves, which differs greatly depending on the interests of those concerned: the Americans have estimated them to be about 200 billion barrels, an exaggerated figure it seems , to encourage investment in the area and put pressure on OPEC (mainly to avoid rising oil prices), instead, the assessments of Russia and some Western companies with interests in other regions (e.g. British Petroleum) circulate figures below 50 md. barrels[14].

There has been a dramatic increase in interest in Caspian hydrocarbons, not only from strategic actors, driven by reasons such as: the desire of the West (mainly the EU and the US) to reduce dependence on the Middle East, the increased interest of Asian strategic actors such as China and Japan, for the Caspian hydrocarbons, plus the fact that the Caspian Sea area has become the meeting place and confrontation of the spheres of influence of the two great powers, Russia and the USA.

The essence of the Caspian "game" lies both in the control over the production of oil and natural gas, and, especially, in the control over the pipelines through which the hydrocarbons will be transported to the world markets[15]. This resulted in another classification of actors in the region: *oilers and gamers*.[16]

The abundance of hydrocarbon resources in this area, the interest and influence of major international actors (USA, Russia, China, EU), but also some regional ones (Turkey, Iran), as well as the interest of states wishing to benefit from the transit of energy resources on their territory - including Romania - include the Caspian Sea area among the main regions of economic and geopolitical interest, with the potential to generate tensions and even conflicts, caused by the divergent interests of different actors"[17].

5.5. The Black Sea – a sea of conflicts

Quiet almost the entirely period of the post-World War II, until the events in Central and Eastern Europe (1989-1991, including the dissolution of the Soviet Union), the Black Sea area became the most conflictive in the world, both with frozen conflicts, as well as open conflicts, as we demonstrated in a previous study[18]. We recall only the conflicts in the former Yugoslavia (especially in Bosnia and Herzegovina and Kosovo), the Caucasus (Chechnya, South Ossetia, Abkhazia, Nagorno Karabakh), the Republic of Moldova (Transnistria).

Although is quite large (413,488 km2), the Black Sea has only three geostrategic points, but really relevant: *the Bosphorus and Dardanelles straits*, which connect the Mediterranean Sea and, further, the Planetary Ocean, *the mouth of the Danube* (which provides the connection with the interior of the continent) and *the Crimean Peninsula*, the

[14] Javier Morales (2004), *Reservas y transporte de petróleo en el mar Caspio: el oleoducto Baku-Tbilisi-Ceyhan*, UNISCI, pp. 2-3.
[15] Silviu Neguț (2015*), Geopolitica*, Editura Meteor Press, București, p. 651.
[16] Enayatollah Yazdani (2006), *Competition over the Caspian oil routes: Oilers and Gamers perspective, in "Alternatives Turkish Journal of International Relations",* vol.5, p.51.
[17] Silviu Neguț (2015), *op. cit.*, p. 663.
[18] Silviu Neguț (2013*), Marea Neagră – o mare a conflictelor?*, în vol.*"Conferința Națională a Societății de geografie din România",*24-26 May, Timișoara, 10th edition, Eurobit Publishing House, pp. 926-934.

only important peninsula in the entire Black Sea basin, a geostrategic point of crucial importance for the control of the entire Black Sea basin, as well as of the Azov Sea.

In the Black Sea area itself, there are, in a geopolitical spirit, six actors: a state with super-power claims (Russia), a regional power (Turkey), an actor with claims to regional power (Ukraine), but which has lost this rank (after Crimea was annexed by Russia), and three pawns (Romania, Georgia, Bulgaria), two of them being Euro-Atlantic members.

For the West, as far as the Black Sea area is concerned, the events of 1989-1991 and the end of the Cold War had at least two positive consequences:

- the advancement of democratic regimes to the east, as a result of the integration into the European Union of some former communist states (in this case Romania and Bulgaria, having sea access, others being nearby);
- facilitating access to the vast resources and essential raw materials, especially energy, by interconnecting the Pontic space with the Caspian and Central Asian space (a desired and necessary alternative to Russian resources and transit routes controlled by Russia). Furthermore, the geo-economics dimension of the Pontic space was doubled by the geostrategic, implicit and military (NATO enlargement, implementation of American Anti-Missile Shield components near the Western Black Sea coast, including Romania, as well as the Tailored Forward Presence of American and NATO military forces in the area) and geopolitical (extension of the Euro-Atlantic structures in Moscow's sphere of influence).

However, three decades after the end of the Cold War, the Black Sea area is once again a *gray area*, foreshadowing a possible new Cold War, if not a little more. The events of the last 10-15 years, including the Russo-Georgian War (August 2008), followed by the declaration of independence by the two Georgian autonomous republics (South Ossetia and Abkhazia) – an act immediately recognized by the Kremlin – , the reintegration of Crimea into the Russian Federation (March 2014) and its interference in destabilizing the eastern region of Ukraine by openly supporting pro-Russian rebels, in addition to the slightly older ones (Chechnya, Transnistria).

5.6. Other important Eurasian regions

Apart from those already mentioned, there are other important geopolitical-geostrategic regions, without open conflicts such as those discussed above, among which at least three stand out:

A. *Association of Southeast Asian Nations – ASEAN* (founded in 1967, based in Jakarta), which includes 10 states: Brunei, Cambodia, Philippines, Indonesia, Laos, Malaysia, Myanmar, Singapore, Thailand and Vietnam – most of them involved in the dispute with China over the islands of the seas of South China and East China, which could make the area conflictive at any time. Occupying an area of 4.48 million km^2, it has a population of 664.2 mil. inhabitants (continuously and rapid population growth due to the positive natural increase) and a GDP ppc of 9107 billion. USD.

B. *Shanghai Cooperation Organization – SCO* (founded in 1996 in the "Shanghai Five" formula, later expanded; based in Beijing) includes 8 members: China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India and Pakistan. It is the most important regional association as strengths: area (34.3 M km^2, almost 1/4 of the planet's extent), population (3.16 billion inhabitants, 40% of the world total) and GDP *ppc* (45300 billion USD, of 2.1 times larger than the USA and 2.8 times larger than the EU). The lack of this geopolitical-geostrategic region is represented by the existence of 3 prominent actors (China, Russia and India), each one with its own natural pretension of being its leader, which impedes to impose a coherent program on the world stage.

C. *European Union – EU* (founded in 1957 under the name of the ECSC/Coal and Steel Economic Community, the current formula since 1992). Its strengths are: an appreciable area (4.48 M km2, almost half of the extent of Europe), a significant population (472.6 M inhabitants, 2020, 2/3 of the continent's population), a significant GDP *ppc* (USD 16400 billion, 2019) and a representative as a permanent member of the UN Security Council (France, until recently had 2). Consequently, the EU represents both a relevant geopolitical-geostrategic region and one of the main actors of the Eurasia and, at the same time, the world stage.

But recently, the EU has been hit by a series of events, such as the global economic crisis (triggered in 2008) and Brexit (effective January 1, 2020), which caused it to lose 12.8% of its population and 14.5% of GDP ppc. Terrorism was added (Madrid-11 March 2004, Paris- 7 January and 14-15 November 2015, Brussels-22 March 2016, Nice-14 July 2016, Berlin-14 December 2016, etc) and immigration (in 2018, 2.4 M immigrants from outside the EU -27 entered, and on January 1, 2019, 21.8 M people from outside the EU-27 were registered in the EU-27). For some time, it has been affected by the lack of cohesion, manifested among others, by: the establishment of a hard core, Framany (France + Germany), "Europe with more speeds", "Europe of the regions", the differences of accent on the dominant feature of the Union (economics-German vision; politics-French vision), the absence of a unitary position on essential issues such as gas pipeline projects Nord Stream and Nord Stream 2, the wave of immigrants from the second decade of the 21st century, the Chinese project "The New Silk Road", etc. Another weakness is the blocking of the enlargement of the Union after the acceptance of Croatia (2013), the process can be continued in the Western Balkans, Eastern Europe and the South Caucasus, but less (at least in the near future) in Turkey (the country with the old candidacy).

6. The New Silk Road: One Belt, One Road – the project that unites or devides Eurasia?

As the Chinese call it, "The 21st century Project", officially inaugurated in May 2017, *the New Silk Road* is a much greater initiative, than *the Old Silk Road* or any other economic project ever proposed.[19] As the name indicates, *One Belt, One Road Project*, it owns two different branches. *The Belt*, the land-based route follows the Old Silk Road (similarly starting from the ancient Chinese capital of Xian, however ending not in northern Africa, but in Europe's greatest North Sea port, Rotterdam) and having many ramifications along the way(one of them pointing to the Romanian port of Constanta, the largest port by the Black Sea). *The Road*, the oceangoing route leaves Zhanjiang a port city by the South China Sea, in South-Eastern China – chosen, among other assets, thanks to its geographical position, located near 3 major urban and economic metropolises (Guangzhou/former Canton, Hong Kong and Macau) – and going down the route of Malacca Strait – the Indian Ocean-Suez Canal, arrives in Europe, ending its journey with the terminus Mediterranean city ports of Athena (Piraeus) and Venice.

In the meantime, a third branch has been added, namely *the Iron Road of Silk*, a railway network (31,000 km long and crossing 29 countries) that connects the major cities of Shanghai (China) and Rotterdam (Netherlands). In fact, in 2019, the first uninterrupted railway transport between Xi'an (the starting point of the New Silk Road) and Istanbul, on the Black Sea, has already been built.

[19] For details see Silviu Neguț, Marius Cristian Neacșu (2017), *The new Silk Road: One Belt, One Road- a strategic Power Asset for China, in "The Complex and Dynamic Nature of the Security Environment",* "Carol I " National Defence University Publishing House, Bucharest, pp. 81-88.

Although crystalized stand points (opposing or favoring the idea) are somehow premature, it is nevertheless possible to distinguish, at least, a tacit agreement coming from the countries, which will benefit from concrete visible direct investments, but we may just as clear notice the restrained attitude of some important regional stakeholders (India, Japan, European economic powers) or global stakeholders (mainly USA).

Depending on the events that could take place in the two big powder kegs/ cauldrons (South China Sea and East China Sea), it would be possible for other countries to protest against the project. Also, other countries that will feel restricted in their economic decision-making power due to the Chinese "encirclement". So, in time, it is possible for *the New Silk Road* to divide Eurasia.

Conclusions

First of all, Eurasia is the largest continental mass on the planet in terms of area, population and economic power. At the same time, it concentrates most of the geostrategic players who, individually or in certain combinations/alliances, try to control the huge geopolitical ensemble that has individualized in time or a large part of it, not infrequently causing conflicts with large-scale effects. At the same time, we must not forget that the United States, still the only global power, has great interests in Eurasia and is fully involved in it.

Also, in parallel, some regions/areas have been individualized over time, let's say, geographical areas with a series of common natural, civilizational, historical-geopolitical, economic characteristics, etc. which, especially in modern times, but also today they are hot, conflicting areas, with effects on large areas, even globally. Of these, we focused on a few: the Middle East, the Korean Peninsula, the Balkans, the South China Sea, the East China Sea, the Caspian Sea, the Black Sea.

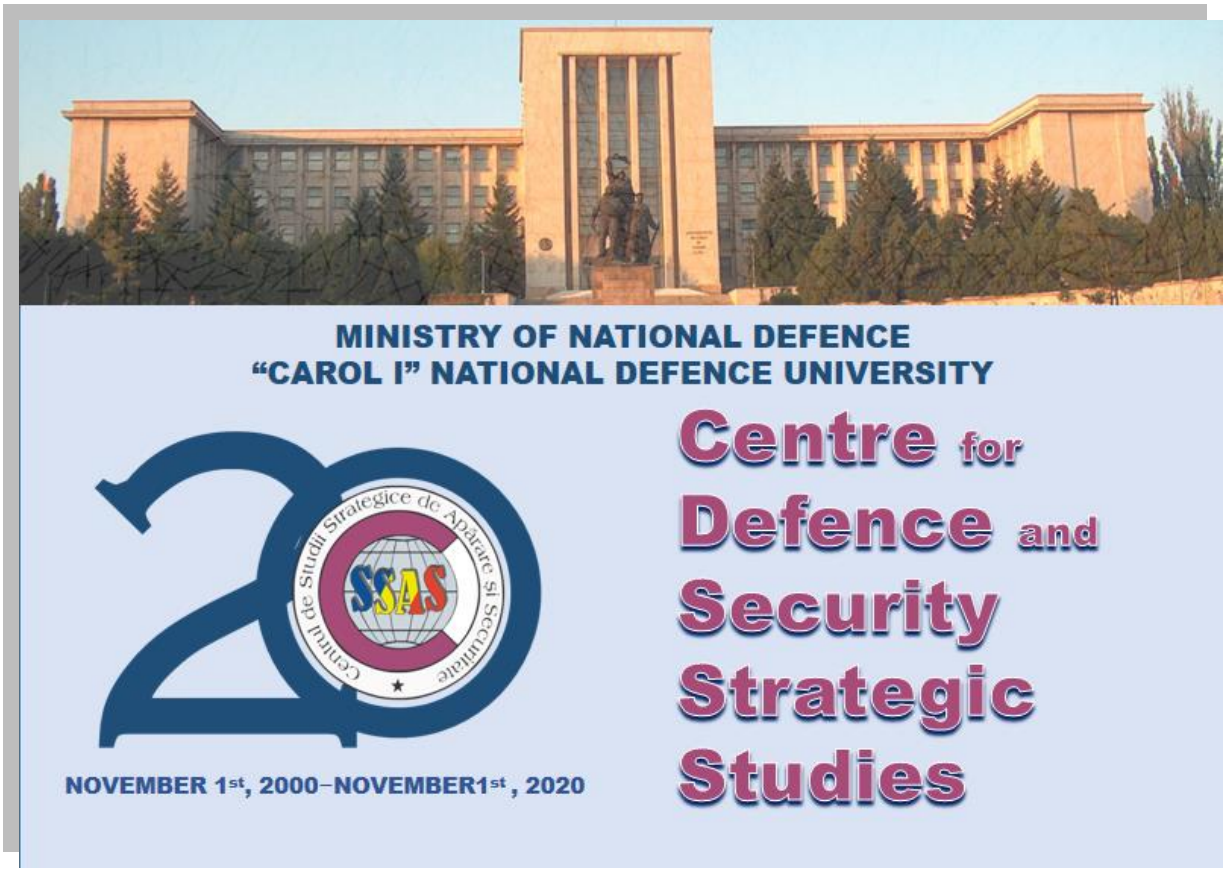
Eurasia is also home to the largest economic project of the 21st century, *the New Silk Road*, of an extraordinary scale. However, this project has ambivalent values, being still difficult to distinguish between the desire of the great power in growing China to "encircle" the Old World economically and, respectively, the advantages for each country in part of those involved in the project.

BIBLIOGRAPHY:

1. ***, *Britannica: Book of the Year 2019; CIA. The World Factbook 2020:* https://www.cia.gov/library/publications/resources/ the-world-factbook/index.html
2. ***, *Calendario Atlante de Agostini 2020*, Instituto Geografico de Agostini.
3. ***, *SIPRI Yearbook 2019*: Armaments, Disarmament and International Peace Research Institute, URL: www.sipri.org/databases
4. ***, *United Nation Statistical Yearbook 2019*, URL: https://unstats.un.org/unsd/publication/ statistical -yearbook/files/syb62/syb62/.pdf
5. BRZEZINSKI, Zbigniew, *A doua șansă. Trei președinți și criza superputerii americane*, Editura Antet XX Press, Filipeștii de Târg.
6. CHAUPRADE, Aymeric; Thual François (2004), *Dicționar de geopolitică: state, concepte, autori*, Editura Corint, Bucharest.
7. COUTAU-BÉGARIE, Hervé (2008), *Traité de Geostratégie*, ed. VI-a, Editura Economica, Paris.
8. DEKMEJIAN, Hrair R.; SIMONIAN, Hovann H (2003), *Troubled Waters: The Geopolitics of the Caspian Region*, I.B. Tauris.
9. DOBRESCU, Paul, *Crizele de după criză. O lume fără busolă și fără hegemon*, Editura Litera, Bucharest, 2016.

10. DUGHIN, Aleksandr, *Bazele geopoliticii și viitorul geopolitic al Rusiei*, Editura Eurasiatica.ro, Bucharest, 2011.
11. HARARI, Yuval Noah, *21 de lecții pentru secolul XXI*, Polirom, Bucharest, 2018.
12. KAPLAN, Robert D., *Butoiul cu pulbere al Asiei. Marea Chinei de Sud și sfârșitul stabilității în Pacific*, Editura Litera, Bucharest, 2016.
13. KAPLAN, Robert D., *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*, 2012.
14. LACOSTE, Yves (sous la direction de ~; 1995), *Dictionnaire de géopolitique*, Flammarion, Paris.
15. MACKINDER, Halford John (1904), *The Geographical Pivot of History*, The Geographical Society, vol. 23, nr. 4.
16. MACKINDER, Halford John, *Democratic Ideals and Reality. A Study in the Politics of Reconstruction*, Henry Holt & Co, New York, 1919.
17. MATEI, Horia C.; NEGUȚ, Silviu; NICOLAE, Ion, *Enciclopedia Statelor Lumii*, Ediția a 16-a, Editura Meronia, 2020, Bucharest.
18. MORALES, Javier, *Reservas y transporte de petróleo en el mar Caspio: el oleoducto Baku-Tbilisi-Ceyhan*, UNISCI, 2004.
19. NEGUT Silviu; NEACSU, Marius Cristian, *The New Silk Road: One Belt, One Road - a strategic Power Asset for China*, in *"The Complex and Dynamic Nature of the Security Environment"*, "Carol I" National Defence University Publishing House, Bucharest, 2017.
20. NEGUȚ, Silviu, "Marea Neagră – o mare a conflictelor?", in "Conferința Națională a Societății de Geografie din România", 24-26 mai, Timișoara, ediția a X-a, Editura Eurobit.
21. NEGUȚ, Silviu, *Geopolitica*, Editura Meteor Press, Bucharest, 2015.
22. PARVULESCO, Jean, Vladimir Poutine et l'Eurasie, *Les Amis de la Culture Européenne*, Paris, 2005.
23. SPYKMAN, Nicholas John, *America's Strategy in World Politics. The United States and the Balance of Power*, Harcourt, New York, 1942.
24. YAZDANI, Enayatollah, "Competition over the Caspian oil routes: Oilers and Gamers perspective", in *"Alternatives Turkish Journal of International Relations"*, vol. 5, 2006.
25. ZAKARIA, Fareed, *Lumea postamericană*, Editura Polirom, Iași, 2009.

CDSSS – 20 YEARS OF ACTIVITY



Centre for Defence and Security Strategic Studies represents the forefront of scientific research in the field, having a tradition and prestige recognized both national and abroad, promoting activities and an impressive portfolio of high-scientific papers.

Mission

CDSSS aims to meet the strategic challenges of the contemporary security environment and military science as a whole, through the development, implementation and dissemination of knowledge and research results, active-participative presence in the national and international scientific research arena and, not least, being engaged in the education process of ROU NDU and providing advice and specific support to institutions and organisations in the field of security and defence.


RESEARCH PROGRAMS
SECURITY AND DEFENCE CONCEPTS AND THEORIES
EUROPEAN AND EURO-ATLANTIC SECURITY
AREAS OF STRATEGIC INTEREST
More than 160 scientific research papers
More than 10 strategic analyses
MILITARY STRATEGY
ARMED FORCES AND SOCIETY


SCIENTIFIC EVENTS AND PERIODICAL PUBLICATIONS
More than 20 Workshops
Over 30 International Scientific Conferences and Seminars
Over 40 Public Lectures
STRATEGIC IMPACT
IMPACT STRATEGIC
COLOCVIU STRATEGIC
Strategic Impact is the bilingual academic open access quarterly, indexed in 5 international databases
Strategic Colloquium, indexed in 3 international databases

COOPERATION AT NATIONAL LEVEL

CDSSS provides objective, rigorous and timely analysis both to decision makers within Ministry of National Defence (MoND) and other institutions with responsibilities in the field of national security and defence, as well as support to the education process at strategic level, performed within the "Carol I" National Defence University.

INTERNATIONAL COOPERATION

Over time, CDSSS has signed protocols with international institutions from EU and NATO member states and partners, materialized through joint projects, working visits, participation in conferences, exchange of publications.

INDEX OF AUTHORS

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Director: Colonel Alin CRIVINEANU

The publications consists of 382 pages.

"Carol I" National Defence University Printing House
Panduri Street, no. 68-72, 5th district, Bucharest
E-mail: editura@unap.ro
Phone: 00-40-021-319.48.80/0215; 0453

1643/21.12.2020 C. 286/2020