“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

December 9-10, 2021

Editors
Florian CÎRCIUMARU, Ph.D.
Constantin-Crăișor IONIȚĂ, Ph.D.

“CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, Romania

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

CONTENTS

SECTION I
PANDEMIC CHALLENGES ON SECURITY

SECTION II
STATE AND NON-STATE ACTORS IN POWER RELATIONS

SECTION III
NATIONAL DEFENCE AND RESILIENCE

SECTION IV
STRATEGIC CONCEPTS AND THEORIES

SECTION V
AREAS OF STRATEGIC INTEREST

SECTION VI
INTERNATIONAL HUMANITARIAN LAW

SECTION VII
MILITARY HISTORY

DOI: 10.53477/2668-6511-22-01

SCIENTIFIC SECURITY AND THE BACKBONE OF THE FUTURE ROMANIAN ARMED FORCES

Iulian CHIFU, Ph.D.,
Associate Professor, "Carol I[st]" National Defence University, Bucharest, Romania.
E-mail: keafuyul@gmail.com

Abstract: *Scientific security enters the forefront of the debates related to the evolution of security and military in the future. In that respect, the backbone of the Romanian Armed Forces should move more to fields of scientific research and technological achievements with direct applications and, maybe, a proper scientific and strategic tool at the disposal of the Chief of Defense. The most important fields of research should come from strategic studies, prospective studies, new technologies and their impact, applied military and security sociology, as well as Informational Warfare and impact studies.*

Keywords*: scientific security; strategic studies; prospective studies; informational warfare; impact studies.*

1. Scientific Security: how to securitise science?

Scientific security as a field of interest for securitisation is floating around for some time. But this has never come as a natural concept, since the idea of securitising any piece of a field where creativity and inventively are the leading characteristics seems impossible. But, on another point, huge steps have been made in opening the way for technological security, and that's a step forward. Moreover, the fact of protecting copyrights, licenses, brevets, research has already been a concern, even though this is far from the real meaning of scientific security which aims, according to our concept, to deal with the evolution of research, of theorisation, protecting them and inducing rules and norms according to common interests, shifting realities and perceptions and framing new markets as well as new environments for the new adapted World Order.

In that respect, we will refer here to the technological security, already a concept well developed and used, and which already enshrines more than technology, adding also research in fundamental fields, strategy and strategic thinking, prospective studies, horizon scanning and future studies, as well as important concerns in the sociological security field as in the impact studies as well as consequence management studies. We will also add the inputs that gave the scientific security new impetus coming from the recent QUAD[1] summit and the ways to approach China for a soft containment, as well as the transfer of technologies and instruments to deal with Beijing in the AUKUS[2] framework.

For us, the main fields of interest in scientific security would be: strategic studies/strategies and strategic thinking; prospective studies/horizon scanning/future studies; new technologies and their impact on the human being, society, politics, international relations and global security; impact studies and consequence management for the decisions so that they

[1] A.N.: The Qadrilateral Security Dialogue in the Indo Pacific, a format between the US, India, Japan and Australia founded in 2007 at Japan's proposal, reestablished in November, 2017.
[2] A.N.: A trilateral security pact between Australia, the United Kingdom and the United States, announced on 15 September 2021 for the Indo-Pacific region.

could not lead to man-made crisis; applied military and security sociology, the knowledge of the real society we are living in and attractiveness for the military service as well as the synergy of sociological cultures of people involved in the defense field – order, rigour, strict vertical of power versus hazard, random behaviour and special needs and millieux for computer, IT and cyber researchers and drone operators as well as creativity bubbles, music and silence for researchers in fundamental studies; Informational Warfare and study of perception and channelling perception formation towards a desired goal.

A very important reference in this direction is the US National Technology Security, a US Government supported initiative by a grant from the U.S. Air Force Office of Commercial and Economic Analysis (OCEA). The project, run by the Center for New American Security (CNAS), is aiming at far more that technological security, and, according to the objectives of the project, it will develop the intellectual framework for a national technology strategy for a successful, long-term American innovation and technological leadership through policies for accelerating American innovation, mitigating risk to US advantages, and contending with the technology strategies of competitors (The Center for a New American Security - CNAS. 2021).

The project is a clear reflection of the scientific security since it will also explore options for boosting innovation through research and development funding, developing and maintaining human capital (STEM education, high-skilled immigration, upskilling), technical standard-setting, and supplying public goods (data, computing resources). This project explores the institutional and bureaucratic processes through which the government should develop and execute an effective national approach. This project analyses measures such as increased supply chain diversity and security, improved visa screening, targeted export controls and investment screening, and increased and more effective counterespionage investigations (U.S. National Technology Strategy).

2. Technological security as a part of Scientific security

In order to launch the debate about technological security as part and parcel of the scientific security, we've analysed the main strategic documents of the US, NATO, EU, UK, as well as the Report on World Economic Forum from 2021. We've done so looking at the American strategic documents (President Joseph R. Biden Jr. 2021; Annual Threat Assessment of the US Intelligence Community 2021; America's Place in the World 2021; A Foreign Policy for the American People 2021; Global Trends 2040. A more contested World 2021) (Biden National Security Strategy hasn't appear yet); NATO strategic documents and assessments (The Secretary General Annual Report 2020; NATO 2030: United for a New Era 2020; NATO 2030: new technologies, new conflicts, new partnerships 2021); EU strategic documents (Fontelles 2021; The geopolitical implications of the Covid-19 pandemic 2020) – of the High Representative for Foreign Policy, another one from the Foreign Affairs Committee – AFET – of the European Parliament; two British strategic documents – along them the integrated Strategy till 2030, the one supporting the idea of a scientific security per se, since it grants UK the status of Technological and Scientific Superpower until 2030 (Cabinet Office 2021); and finally, the Report of the World Economic Forum (World Economic Forum 2021), The Global Risks Report 2021.

Those documents introduce different concepts and nuances of interpretation, a direct proof that the field involving technological security, not talking about scientific security, is still on the making. The concepts presented in those documents are: scientific power, emerging and disruptive technology, technological supremacy, technological advantage, technological and scientific leadership, technological superiority or development, all could be found in these documents. Moreover, the self-assumed status of scientific and technological superpower by

the Great Britain document is of first importance; it is also about the side effects of technology as it is about the strategic advantage (coming from the technological development); about both technological and scientific power and rapid technological change that transforms science and technology in a modality to measure the power.

In spite of different concepts and nuances in addressing this sphere of understandings of the thematic linked to technological security, there is a convergence of the approaches based on several pillars (Chifu 2021 - 1, 13 - 23):

– science and technology become multipliers and referentials for power, at a global level;

– there is a real competition on research and access to technology, that could lead also to wars and limits of the development widening of the differences on economic growth and development and even creating possibilities for niche developments in the emerging economies that could resettle global hierarchies;

– technology is an advantage and creates opportunities, but could also be a subject of vulnerability for an actor and source of threats for the mankind;

– technology polarises and creates alliances for technological exchange as well as constraints, containment, limitations for the access to technologies or for the alternative options for the sources of technology;

– the space that usually is referred as technology implied in the area and could also be found in technological security, as in science and scientific security, refers also to IT, artificial intelligence, cyber, nano-technologies, biotechnologies, big data, quantum computers, space technology;

– we do not have in hand or in the international law norms and ethical limitations for the exponential development of new technologies, which could turn out to be-disruptive or even destructive technologies;

– chassing new technologies could mean, in the case of an autocracy, the race towards a kind of supreme weapon, used to dominate the World;

– we do have enemies already identified, not only technological or scientific competitors, since those actors or countries aim at dominating the World, absolute control, or channelling and constraining our normal way of thinking. China and Russia are considered here, each with its own merits, nuances and major differences between the two actors concerning the degree of identified danger each of them are representing for us.

As we have seen before, technological security is just a slice of the scientific security. In the other part are situated the rights and values of the ethics of research, but also securing money for the research, genuine discovery and respecting the copyrights and primacy in discovery in the scientific research. It is also about fair competition and correct attribution of merits in the research, but also the very pragmatic ways to get to targeted results in the scientific research, combined with the legitimacy and opening in accepting the side effects of a discovery and the impact study, as well as the consequences of such a leap into knowledge or the effects of the excessive use of a technology or discovery without accepting its limits and by-products that need to be also addressed and presented in full transparency.

The ethics of using scientific research are a completely different and difficult subject since, in some cases, the technology is used in a different direction then a virtuous constructive one: limiting human rights, controlling the ways of thinking or the behaviour of individuals all over the world, not only on a nations' own citizens; as on another point, there are ways to control, limit or monopolise the ingredients or needed parts, if not the knowledge, instruments of research and means to build critical technologies, or it is possible to completely ban the access to specific technologies for some states. As we could see, the complexity of scientific security is far broader.

3. QUAD and AUKUS as frameworks for technological transfers and sources of scientific security

QUAD recent first in person summit, held at the White House, with the chiefs of state and governments of the four member countries – US, Japan, India, Australia – has brought a new impetuous for scientific security, with different uses. Created with the purpose to contain China, a type of soft containment, as we put it (Chifu 2021 - 2), the institutionalisation of the agreement and deepening of the links came with an impetus for practical cooperation that includes also technological transfers or common efforts for: ending Covid-19 pandemic (the first official global document where this formulation appears, as well as the final deadline, 2022), including research in this field with security impact; rising the production and access safe and effective vaccines; promoting high standards infrastructure; fighting climate crisis; partnership on emerging technologies, space and cyberspace (The White House 2021 - 1). All include pieces of scientific security and in the subtext is referring to China, China's behavior and Chinese responsibility.

At the same page are the references to build a global pandemic radar and fight future pandemics, even though the document does not mention any responsibility of China for the Covid-19, or an appeal for a correct and in depth investigation of the first moments of emergence of a pandemic. High standards, transparency in constructions, high standards and Build Back Better World (B3W) – as an alternative programme to One Belt One Road project is also about scientific security, technological security and compete China at a different level including a different approach to quality as a difference from cheap and low quality infrastructure attributed to China. It comes also with a green component of the infrastructure build by the QUAD and assistance to third countries in the region. Green ports and green corridors in the Indo-Pacific region is also a challenge to China's dominance in the region, with an added value. As it is the case with the clean energy, controlling emissions, decarbonisation and how to reach this through innovation, adaptation, resilience and preparedness in front of civil emergencies created by extreme weather.

Last but not least, in the field of scientific security, there's a new innovation about finding, agreeing and using common standards and norms between QUAD states and their partners. This comes also from new discoveries in the technological field through scientific research in a technological ecosystem open, accessible and safe in order to create competitive standards, diversify 5G sources and providers, creating correct chains of suppliers and technology and developing horizon scanning – needed studies for anticipation and preparedness. As is the case with emerging and disruptive technologies that need to be subject to control and respect for the democratic values and human rights, another standard that forfeits Chinese competition.

A declaration of principles of the QUAD on standards to design, develop, govern and use technologies is another important tool for the soft containment of China using just diplomatic approaches and technical and scientific achievements (Chifu 2021 - 2). A new form of technological and scientific security comes exactly from the standards imposed and observed globally in several domains. Advanced telecommunications, artificial intelligence, chain of providers safe for semiconductors and monitoring of the evolutions in biotechnologies are also pieces that could be assumed under the framework of scientific security.

As interesting as the QUAD final document, related to technological and scientific security, is the approach to military assistance and technological transfer from the US and UK to Australia, via the AUKUS agreement. Sitting in the framework of the China soft containment, the assistance for Australia and the global fight of democracies against autocracies as the QUAD, the AUKUS prove to give birth to numerous miss-understandings with France and the EU (Chifu 2021 – 3). But it also represents a huge transfer of technology and an important instrument of scientific security in support for Australia, but also holding an

important significance for South China Sea region and Taiwan. As it announces support for the small island states from the Pacific, all being subject to different types of pressure from China (The White House 2021 - 2).

This agreement noted the coordination of signatories in cyber area, in advanced technologies for the defense, first and foremost in nuclear propulsion for submarines – the first transfer of sensitive technologies in the last 50 years and plus. But it involves also other capabilities and submarine activities, instruments against modern security submarine challenges including first hand key technologies of primary importance for the effectiveness of the military activities of the future: artificial intelligence, disruptive technologies from the cyber sphere, and high precision capabilities with long range (The White House 2021 - 2), all with an important content of scientific research and accomplishments, another component of the proposed concept of scientific security.

4. Scientific security and research in Russia: EW and autonomous and robotic systems for modern warfare

The concerns are not at all trivial since, on the other side, the investments and achievements are important in the technological and scientific fields. We will only discuss here about some achievements of Russia, since the scientific literature confirms this approach to scientific security that Russian Army holds. And we will look at two directions, electronic warfare and unmanned robots. The lessons learned are coming from the last Zapad 2021 exercises and presentation of the new achievements, but also the integration of those technical and scientific projects in the warfare landscape.

Electronic Warfare (EW; in Russian, *radioelektronnaya borba*, or REB) has involved forming specialist EW structures, including at the brigade level, and populating all branches and arms of military service with EW-trained personnel and equipment. It targets capabilities to disrupt, jam and interfere with potential enemy command-and-control (C2) systems, communications, radars, or weapons (Petrenko 2021). EW assets entering service over the past four years, are dominated by Divnomorye-U offering EW protection from radar reconnaissance across an area of several hundred kilometers by generating an "umbrella" of EW interference. The EW complex detects and then analyses the target signal and type, alongside its power and direction of radiation, using artificial intelligence (AI) for suppression plan and selection of the most effective jamming methods (McDermott 2021).

According to military specialists (Vitaly 2021), The Divnomorye-U is designed to emit high-powered radiation that neutralizes enemy radar, regardless of type. It is reportedly capable of jamming both ground-based radars and radars of aircraft such as E-8 JSTAR, E-3 AWACS, E-2 Hawkeye, as well as radar equipment aboard helicopters and unmanned aerial vehicles (UAV) (Nikiforov 2021) EW capabilities were made public in late 2017 by then–deputy defense minister Yury Borisov. This related in particular to the Palantin, Rtut-BM and the Tirada-2S systems proving a level of knowledge implying scientific security that could influence any future NATO-Russian conflict (McDermott 2021).

At the same time, Zapad military exercises have proven another capability, the Russian unmanned robots. Russia has employed unmanned ground vehicles in combat formations for the first time, a significant step in the country's quest to develop an effective all-robot military unit, experts say. Two remote-controlled vehicles have been presented, according to Russia's Defense Ministry statement (Wellman 2021): The Uran-9, a tracked vehicle equipped with a 30 mm autocannon, a machine gun, anti-tank missiles and a flamethrower and the smaller Nerekhta unmanned ground vehicle, firing at targets with a mounted machine gun and a grenade launcher. Both were used for fire support and reconnaissance work, performing tasks that would be dangerous for troops, such as delivering ammunition and equipment in combat, seeking to

obtain greater lethality and survivability. Other machines were being used for mine clearing and urban warfare.

5. Lessons learned for the Romanian Armed Forces

The Romanian Armed Forces should consider those evolutions in technological and scientific security and try first to create an understanding on the field. Theoretical approach and a full presentation of the content of both concepts, especially scientific security, should be of first importance. Then, an update of existing instruments and an assessment of what the Romanian military needs, in terms of technology, research, strategies and capabilities should come up, in a different scientific transdisciplinary program.

Coping with the difficulties of building up such capabilities and preparing the institutional framework would be next, including the consequence management of this development and problems with integrating different cultures in the military framework. And here, too, the MoD should allocate at least 2% of its budget to scientific research of this kind.

It is clear that the Chief of Defense and appropriated bodies should consider to develop a proper scientific and strategic tool at their disposal, to be integrated in the existing institutional framework and chain of command, but allowing resources to reach this project and launching the proper interface to engage, attract and hire human capabilities, experts and needed minds, in a transdisciplinary effort, in order to achieve such an important objective.

BIBLIOGRAPHY:

BIDEN Joseph, R. Jr. (President). 2021. Interim National Security Strategic Guidance, March 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

BLINKEN Antony J. 2021. America's Place in the World. 4 February. URL: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/

BORRELL, FONTELLES, Joseph. 2021. European Foreign Policy in Times of Covid 19, Luxembourg: Publications Office of the European Union, 2021, ISBN 978-92-9238-927-7. URL: https://www.euneighbours.eu/sites/default/files/publications/2021-03/european_foreign_policy_in_times_of_covid19.pdf

Cabinet Office. 2021. Global Britain in a Competitive Age. The Integrated Review of Security, Defence, Development and Foreign Policy. URL: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

CHIFU, Iulian. 2021 - 1 Securitate tehnologică. Un nou domeniu de strictă actualitate a securității viitorului, Revista Infosfera, nr 2/2021: 13-23, ISSN 2065-3395.

CHIFU, Iulian. 2021 - 2. Îndiguirea soft a Chinei: de la Război Rece la schimbarea piețelor, standarde și comportamente alternative. Adevărul, 27 September 2021. URL: https://adevarul.ro/international/asia/Indiguirea-soft-chinei-razboi-rece-schimbarea-pietelor-standarde-comportamente-alternative-1_6151555a5163ec4271af690b/index.html

CHIFU, Iulian. 2021 - 3. Pentru un contract ratat cu submarine, Franța împinge UE spre confruntare transatlantică, Adevărul, 20 septembrie 2021. URL: https://adevarul.ro/international/europa/pentru-contract-ratat-submarine-franta-impinge-ue-confruntare-transatlantica-1_614813845163ec42716ddb20/index.html

EU. 2020. The geopolitical implications of the Covid-19 pandemic. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/603511/EXPO_STU (2020)603511_EN.pdf

McDERMOTT, Roger. 2021. Russia's Military Boosts Electromagnetic Spectrum Capability, Eurasia Daily Monitor. Jamestown Foundation. Volume 18. issue 144. 22 September 2021. URL: https://jamestown.org/program/russias-military-boosts-electromagnetic-spectrum-capability/

National Intelligence Council. 2021. Global Trends 2040 - A more contested World. URL: https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

NATO. 2020. NATO 2030: United for a New Era. 25 November. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO. 2021. February. NATO 2030: new technologies, new conflicts, new partnerships. URL: https://www.ndc.nato.int/news/news.php?icode=1527

NIKIFOROV, Sergey. 2021. The three most important technologies of the Russian Armed Forces in recent years are named. Politexpert.ru. 4 June 2020. URL: https://politexpert.net/199331-nazvany-tri-samye-vazhnye-tekhnologii-vs-rossii-poslednikh-let

Office of the Director of National Intelligence. 2021. April. Annual Threat Assessment of the US Intelligence Community. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

PETRENKO Olga. 2021. "Sobering signals": the US is looking for ways to combat Russian electronic warfare systems, 25 January 2021. URL: https://discover24.ru/2021/01/otrezvlyayuschie-signaly-ssha-ischet-sposoby-borby-s-rossiyskimi-kompleksami-reb

PHILLIP, Walter, Wellman. 2021. Zapad military drills showcase Russian unmanned robots' battlefield breakthrough, Stars and Stripes, September 15, 2021. URL: https://www.stripes.com/theaters/europe/2021-09-15/russia-robots-war-games-zapad-ugv-2897317.html

The Center for a New American Security - CNAS. 2021. U.S. National Technology Strategy. URL: https://www.cnas.org/u-s-national-technology-strategy

The Secretary General Annual Report. 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf

The White House. 2021-1. Fact Sheet: Quad Leaders' Summit, September 24, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/

The White House. 2021-2. Joint Leaders Statement on AUKUS, September 15 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/

US Departament of State. 2021. 3 March. A Foreign Policy for the American People. URL: https://www.state.gov/a-foreign-policy-for-the-american-people/

VITALY, Orlov. 2021. War is invisible and effective. Voyenno Promyshlennyy Kuryer, 24 August 2021. URL: https://vpk-news.ru/articles/63516

World Economic Forum. 2021. The Global Risks Report 2021. 16th Edition, ISBN: 978-2-940631-24-7. URL: http://wef.ch/risks2021

DOI: 10.53477/2668-6511-22-02

MEASURING GOVERNANCE AND ASSESSING TRENDS IN DEMOCRACY DURING TIMES OF PANDEMIC

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: *Bringing to attention the main theoretical landmarks regarding the national governance is a necessity since there are heated debates on the role of the state in the management of phenomena that transcend its borders such as international migration and the COVID-19 pandemic. In this context, the paper aims to carry out a non-exhaustive analysis, but focused on recent trends in the study of governance, correlating them with the latest events and determining phenomena that manifest themselves in the international security environment. The goal is to determine whether or not and to identify how the pandemic has influenced governance as a whole, the decline of democracy in particular, as well as national security, especially in the case of European states.*

Keywords: *governance, good governance, decline in democracy, illiberalism, COVID-19 pandemic, national security.*

The last decade has emphasized the challenge of good governance, both as a necessity and, correlated, as a principle and value. The contexts are varied: from the spread of liberal autocracies or so-called "illiberal democracies" to the crisis triggered by international migration or the COVID-19 pandemic. The development of these crises has shown that there is a need to strengthen governance as a key lever for sustainable development and systemic resilience. Internationally, for at least the last two years, the pandemic has highlighted the need for effective cooperation between states, but the issue of growing differences between forms of government has hampered the effective management of the crisis and has given rise to new tensions and to a real competition between countries. Overall, the pandemic has exacerbated several negative trends in the international security environment, including questioning the ability of multilateral institutions to manage the crisis, weakening governance, democratic backsliding, increasing US-China rivalry that faced Europe with a difficult strategic choice. Therefore, at least for the time being, it cannot be said that the COVID-19 pandemic was a catalyst for international cooperation, but, on the contrary, many countries have focused on the national level (see measures to restrict exports of materials considered vital for crisis management and the temporary closure of borders). At this level, too, governance has not been an easy task, with the pandemic causing a number of challenges through subsequent crises: from health to economic and social ones.

1. Governance and democracy. A theoretical framework

Governance is the framework set by the government to ensure the optimal functioning of the state, it is the way a government implements its policies to achieve the desired objectives. Instead, the government represents those forms of command and control characterized by the role of central public institutions, hierarchical relations, electoral responsibility, legal

instruments, and binding decisions applicable to all (*erga omnes*) (Bartolini 2011). In a classical approach, the role of the national government is to ensure that the demands and needs of citizens, voters, consumers and taxpayers are transferred and aggregated by the political system that generates a response through its policies, then implemented by the public administration (Bartolini 2011). Governance depends on the government, the latter promoting various types of policies, rules and regulations based on its form (democratic, autocratic, totalitarian, etc.).

At the national level, governance is defined as the exercise of economic, political and administrative authority to manage a country's problems at all levels, and includes mechanisms, processes and institutions through which citizens and groups articulate their interests, exercise their legal rights, fulfil their obligations and mediate disputes (COTRAIN and UNDP-Philippines 1997, 6). Moreover, the government faces a major challenge: to promote, support and sustain human development understood not only as economic development, but especially as a way to improve human skills (long life and health, knowledge, a decent standard of living) and creating the conditions for development (participation in political and community life, environmental sustainability, human security, rights, gender equality) (HDRO Outreach n.d.). The World Bank identifies the three main dimensions of government: the form of the political regime, the process by which authority is exercised in managing a country's economic and social resources for its development, and last but not least, the ability of governments to design, formulate and implement policies and to discharge functions (The World Bank 1994, xiv).

Francis Fukuyama defines governance by emphasizing the ability of a government to produce and enforce rules, to provide services, whether that government is democratic or not (Fukuyama 2013, 3). He emphasizes that, compared to the goals that governance must achieve, the quality of governance is something different, governance being about the performance of the agents in fulfilling the wishes of those who lead, not about the goals set by them (Fukuyama 2013, 4). Thus, referring to Woodrow Wilson's view of administration, Fukuyama states that government is an institution that can function better or worse, while governance is about execution or public administration, being opposed to politics. For example, "an authoritarian regime can be well governed, just as a democracy can be mal-administrated" (Fukuyama 2013, 4).

If the above elements characterize an ideal of governance, this process nevertheless includes both the good and the bad methods that a society uses to distribute power and manage public resources and problems (Blunt and Rondinelli 1997, 9). By introducing normative descriptors in the definition of this concept, two others appear: good governance and bad governance. The first was advanced in the late 1980s by the World Bank as including "predictable, open, and enlightened policymaking (that is, transparent processes); a bureaucracy imbued with a professional ethos; an executive arm of government accountable for its actions; and a strong civil society participating in public affairs; and all behaving under the rule of law" (The World Bank 1994, vii). UN has been identified key features of good governance: participatory, transparent, accountable, affective, equitable, and promoting rule of law (COTRAIN and UNDP-Philippines 1997, 6) (Quiles 2013).

In the same conceptual framework, bad governance is a consequence of corruption, which is defined as systematic and unpunished violation of the rules of an organization or institution by some members who, by virtue of having a certain authority, use the resources of the organization for purposes different of the formally established ones (Bulai 1998). It should be emphasized that it is not enough to discuss only political or economic-administrative corruption, but also moral and cultural corruption, material and symbolic ones. Expert studies show that, unfortunately, bad governance is more widespread in the world than good governance due to the fact that this phenomenon is encountered in any type of society, from totalitarian to democratic one, especially affecting the services of health and education, but also law enforcement (Rose and Peiffer 2019). Moreover, bad governance is not only associated

with the phenomenon of corruption, but also with policy makers who fail to achieve established goals, inefficiently spending large sums of money from public funds.

However, where does one type of government end and the other begin? What is the connection with democracy?

It is important to note that the most widely used governance indicators are based on the premise that there is a strong statistical correlation between the low level of corruption and the fulfilment of the criteria for achieving good governance. In addition, good governance and democracy, along with economic reforms, are seen as interrelated and mutually supportive aspects of the development process (Joseph 2001). There are also authors who argue that democratic institutions and democratically elected governments are key factors in achieving good governance (Stockemer 2009). Others argue that a democratic system hinders GDP growth, while countries with authoritarian political systems thrive faster than democracies because they are able to instil in the masses the spirit of hard work, sacrifice and obedience (Woo-Cumings (Ed.) 1999) (Chan 2002) (Gregor 1979) (Stockemer 2009, 242-43). Other authors consider the relationship between democracy and economic growth to be positive, the latter requiring legal limitations of arbitrary power, which gives individuals the opportunity to safely draw up plans for their economic future (Przeworski, et al. 2000) (Gerring, et al. 2005) (Mobarak 2005) (Sklar 1987) (Stockemer 2009, 242-43). Finally, another perspective starts from the premise that democracy does not have significant effects on economic growth, economic development depending on the existence of growth-oriented government policies and not on the type of the regime of the country (Alesina and Rodrik 1994) (Alesina, Özler, et al. 1996) (Stockemer 2009, 243).

In "Does Democracy Lead to Good Governance?", Daniel Stockemer, professor of Political Science at the University of Ottawa (Canada), examines the main premises used in governance literature and concludes that while many studies link democracy to more effective public governance, they fail to clearly establish the relationship between the two concepts (Stockemer 2009, 244). This link is also neglected in the case of development studies: while acknowledging the need for democracy, they focus mainly on the relationship between good governance and economic, social and cultural development (Stockemer 2009). Stockemer refers to Mustapha K. Nabli and Charles Humphrey's "Better Governance for Development in the Middle East and North Africa: Enhancing Inclusiveness and Accountability", in which the authors state that the most important conditions for sustainable development and growth are: stability and efficiency of the government in the absence of corruption, the regulatory qualities of the state and the rule of law; at the same time, the lack of effective governance practices reduces the ability of governments to meet the challenges of a globalized world (Stockemer 2009, 244).

In a critical essay on good governance, Merilee S. Grindle, Professor Emeritus of International Development at Harvard, argues that this concept is rather obscure than clear, with so many positive features that it has led to an approach characterized by ambiguity on the role of governance in the development process (Grindle 2016, 1-2). The author states that, for example, two decades ago, the ideal qualities of governments were: effective, accountable, transparent and demonstrating rule of law. Currently, more than 14 conditions need to be identified: equity, participation, inclusiveness, democracy, large-scale service delivery, sound regulation, decentralization, open trade regime, respect for human rights, gender and racial equality, a good investment climate, sustainable use of energy, citizen security, job creation, etc. (Grindle 2016, 2). The link between good governance and development has become a *cliché*, so many analysts believe *a priori* that development requires good governance and good governance leads to development (Hermes, et al. 1999, 43), while the cause-effect relationship is not fully explained. In this regard, Grindle states that there are countries that, although

demonstrating conditions associated with good governance, have not reached a level of well-being, while in many developed and prosperous countries there may be serious governance problems. Thus, governance can improve or deteriorate itself unrelated to the development or well-being of that country (Hermes, et al. 1999). An example is the Ebola crisis in West African countries (2014-2016), in which the media stated that if a country had good governance, it would not have been affected by the epidemic - this statement is considered by Grindle to be erroneous, because it would have been necessary to assess how the country's health care system should have been improved, not the mere assertion of the existence or non-existence of good governance (Grindle 2016, 3). Although theorists continue to critically analyse the relationship between these concepts, the International Monetary Fund states that promoting good governance "in all its aspects, including by ensuring the rule of law, improving efficiency and accountability of the public sector, and tackling corruption" are key elements of the framework in which economies thrive (International Monetary Fund 1996).

The definition of good governance is, in most cases, focused on both the results and the process itself. In this regard, the Organization for Economic Co-operation and Development (OECD) advances the notion of *governance for development* on the premise that societies with more efficient and responsible government institutions perform better on a range of issues, from economic growth to human development and social cohesion (OECD 2012). Governance thus becomes more than a means to development, but even an end in itself (especially in terms of good governance).

Another example is the definition developed by Michael Johnston: good governance consists of legitimate, accountable and effective ways of obtaining and using public power and resources in pursuit of widely accepted social goals, such as legitimate, efficient and responsive institutions and policies, comprehensible processes and results, transparency, incentives to sustain good governance, vertical and horizontal accountability (Johnston 2002, 2, 7-8). The same author also identifies a number of challenges to good governance: avoiding excessive legislation and regulations, giving due weight to policy, building a broad-based support for reform, paying more attention to incentives for leaders and citizens, assessing public opinion, strengthening checks and balances (both administrative, political and political), recognition of resistance to reform, regional approach to issues, and long-term focus (Johnston 2002, 8-14).

It is important to emphasize from this approach the attention paid to the elements of perception and representation: from politics, support for reform and public opinion, to resistance to change, to reform. Therefore, good governance is not just a set of technical desideratum, more or less tangible, but a multidimensional approach in which the citizen and society represent more than the object of governance, but even factors that influence this process.

2. The state and governance as sources of (in) security

Another issue that needs to be addressed is the relationship between government and national security.

According to Barry Buzan and the other representatives of the Copenhagen School, a particular problem can be presented as a threat by framing it either as a special type of policy or as something above politics (Buzan, Wæver and de Wilde 1998). Therefore it can be defined as a spectrum that varies from unpolitized issues, which the state has nothing to do with, to politicization, i.e. the introduction of that issue in public policies that require government decisions and the allocation of resources, and to securitization, in which case the issue is no longer debated as a political one, but it is approached at an accelerated pace and in ways that may violate legal norms and social rules (Buzan, Wæver and de Wilde 1998, 23-6). In this context, it is necessary to clarify the conditions under which governance issues have become

subject to securitization, how they are understood and assessed in terms of influencing security. Therefore, if securitization requires state actors to classify a certain issue as a security one, then the quality of government can also go beyond the scope of politicization and can be included on the security agenda.

Good governance is considered to be the foundation and one of the most important guarantees for national security and, in general, the literature emphasizes the strong correlation between government and national security, referring to the other related concepts: democracy and development (Killion 2014) (Okafor and Malizu 2014) (Hornby 1995) (Bevir and Hall 2011, 356). For example, democracy creates an environment conducive to development, and good governance is essential for sustained economic growth, so it can be said that democratic governance provides the means to reduce socio-economic divisions and tensions affecting the achievement of national security. In a non-democratic system where fundamental freedoms and human rights are not respected, the rule of law is not functioning and participation in governance, justice and fairness is not guaranteed, the national security cannot be achieved. Thus, it is identified a synergistic relationship between national security and democracy (Hornby 1995).

In the event of a pandemic, states are forced to take measures that affect a significant part of the population, causing dissatisfaction, and being subjectively represented as evidence of bad governance or even a decline in democracy, regardless of the values of the indices and indicators presented in the previous section. Moreover, beyond the opinion of population, the COVID-19 pandemic proves that some key-functions of governance can conflict with each other. This is the case for the function of protecting civil liberties and the one of providing public goods to population: free movement and free association are restricted in favour of public health (Alsan, et al. 2020).

Developments in recent years are edifying evidence of Barry Buzan's assertion that "level 2 entities (i.e. the state) act as a source of both threats to and security for individuals, while individuals provide much of the reason for, and some of the limits to, the security-seeking activities of collective units" (Buzan 1983, 18). This statement might be illustrated by two cases that are linked to some of the most important and topical challenges for the European countries: the decline in democracy and the measures taken to manage the COVID-19 pandemic.

In this case, the decline in democracy can be understood in two ways. First of all, the democratic backsliding might be perceived as such by the citizens who are not satisfied with the measures taken by their own government in managing a specific event, such as the pandemic crisis. Second, it can be explained as a decline derived from the direct action of the government in relation with the democratic norms and values. In Buzan's terms, the first case is about the threats arising from domestic law-making and enforcement, but not in the way he explained it ("as a result of inadequate or excessive policing and prosecution practices") (Buzan 1983, 24-5), but as a perverse effect of well-intended legislation that causes dissatisfaction by applying it. The second possible interpretation on decline in democracy brings into forefront the other three general categories of threats emanated directly or not from the state, synthetized by Buzan as: "those arising from direct political action by the state against individuals or groups; those arising from struggles over control of the state machinery; and those arising from the state's external security policies" (Buzan 1983, 25).

The first perspective on decline in democracy links citizens' opinions on the assessed role and efficiency of crisis management measures with the satisfaction with these measures. The Eurobarometer survey shows that a large part of European citizens, around a quarter, felt that restriction measures were not justified (Kantar 2021, 16), and almost half of the Europeans are not satisfied with the measures taken by their national government to fight the COVID-19 pandemic (Kantar 2021, 12).

The second perspective can be analysed focusing on the objective comparison of the crisis management measures with the national and international legislation and democratic values. Beside restrictions on freedom of movement and gathering, still justified by the crisis situation, another example is the case of export restrictions for COVID-19 related drugs and medical supplies: between January and October 2020, 85 jurisdictions around the world enforced such export restrictions despite international calls for cooperation and mutual assistance (The Robert Schuman Centre for Advanced Studies, Global Trade Alert, and The World Bank Group 2020).

If the first perspective has a preponderant subjective component, the second way of understanding the decline in democracy involves measurements by specific indices that also include objective indicators.

Conclusions

From the theoretical framework presented above, some conclusions can be drawn regarding the relationship between government, democracy and national security during the COVID-19 pandemic, as well as how they may evolve. First of all, the relationship between democracy and the quality of governance is not exclusively one-to-one, although, if we look at current Western standards, liberal democracy is the form of government and the political ideology with the best results in terms of economic and social development. Although there is a connection between good governance and development, it involves nuances and a clear definition of terms (good governance, governance for development, development). Governance is, however, a constantly evolving concept, as evidenced by the evolution of both measurement methods (an increasing number of indicators and a multidimensional approach) and its forms of manifestation (e.g., the concept of new governance or global governance). Moreover, the assessment/measurement of the quality of governance must include an objective dimension (basic indicators, mainly of economic and political nature), and also a subjective one (contextual indicators, incorporating previous indicators in socio-cultural contexts: from corruption to of public opinion). Furthermore, security analysis should include a dimension of governance quality analysis, given the strong correlation between governance and democracy.

All these assertions adapt the analysis of governance and security to the current complex and paradoxical context in which, during crises, governments can implement management measures that, on the one hand, will be perceived by citizens as sources of insecurity and anti-democratic measures, and on the other hand, they will come into conflict with each other because, in an attempt to provide public goods to all, governments will be forced to restrict some fundamental rights and freedoms.

It is clear that a pandemic, through the management measures it imposes, can affect both the psychosocial representation of governance and democracy, and their quality. This paper focuses on a number of issues that may or may not contribute to both the decline of democracy and the rise in insecurity. Identifying and studying the indices and indicators for measuring governance and democracy, the sources and causes of insecurity can help to develop policies and implement measures to prevent triggering serial crises.

BIBLIOGRAPHY:

ALESINA, Alberto, and Dani Rodrik. 1994. "Distributive Politics and Economic Growth." *Quarterly Journal of Economics*, 465-490. Accessed November 16, 2021. doi:10.2307/2118470 .

ALESINA, Alberto, Sule Özler, Nourile Roubini, and Phil Swagel. 1996. "Political Instability and Economic Growth." *Journal of Economic Growth*, 189-211.

ALSAN, Marcella, Luca Braghieri, Sarah Eichmeyer, Minjeong Joyce Kim, Stefanie Stancheva, and David Yang. 2020. "Civil liberties during the COVID-19 pandemic." *VOX, CEPR Policy Portal.* 13 November. Accessed November 20, 2020. https://voxeu.org/article/ /civil-liberties-during-covid-19-pandemic

BARTOLINI, Stefano. 2011. "New Models of European Governance. An Introduction." In *New Models of Governance in Europe. Governing in the Shadow of Hierarchy*, by Adrienne Heritier and Martin Rhodes, 1-18. London: Plagrave Macmillan.

BEVIR, Mark, and Ian Hall. 2011. "Global Governance." In *The SAGE Handbook of Governance*, by Mark Bevir (ed.), 352-366. Los Angeles: SAGE.

BLUNT, Peter, and Dennis Rondinelli. 1997. *Reconceptualising Governance.* New York: UN Department of Public Affairs. Accessed November 20, 2021. https://www.researchgate.net/publication/265292783_Reconceptualising_Governance

BULAI, Alfred. 1998. "Corupție." In *Dicționar de sociologie*, by Cătălin Zamfir and Lazăr Vlăsceanu, 141-142. București: Babel.

BUZAN, Barry. 1983. *People, States and Fear. The National Security Problem in International Relations.* Brighton: Wheatsheaf Books Ltd.

BUZAN, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security. A New Framework for Analysis.* London: Lynne Rienner Publishers.

CHAN, Sylvia Sum-yee. 2002. *Liberalism, Democracy and Development.* Cambridge: Cambridge University Press.

COTRAIN and UNDP-Philippines. 1997. *Governance for Sustainable Human Development. An integrated paper on the highlights of four regional consultation –Workshops on governance for sustainable human development.* United Nations Development Programme.

FUKUYAMA, Francis. 2013. *What is Governance?* Center for Global Development. Accessed November 20, 2021. http://www.cgdev.org/content/publications/detail/1426906.

GERRING, John, Phillip Bond, William T Barndt, and Carola Moreno. 2005. "Democracy and Economic Growth: A Historical Perspective." *World Politics*, 323-364.

GREGOR, James A. 1979. *Italian Fascism and Developmental Dictatorship.* Princeton, N.J.: Princeton University Press.

GRINDLE, Merilee S. 2016. "Good Governance, R.I.P.: A Critique and an Alternative." *Governance: An International Journal of Policy, Administration, and Institutions* 30 (1): 17-22. Accessed November 16, 2021. doi:10.1111/gove.12223.

HDRO Outreach. n.d. "What is Human Development?" *UN Development Programme.* Accessed November 20, 2020. http://hdr.undp.org/en/content/what-human-development.

HERMES, Niels, Wiemer Salverda, Herman W. Hoen, and Joachim Ahrens. 1999. "State, Society and Development: Lessons for Africa?" *CDC Research Reports.* Accessed November 16, 2021. https://www.researchgate.net/publication/4785851_State_Society_and_ Development_Lessons_for_Africa

HORNBY, A. S. 1995. *Oxford Advanced Learner's Dictionary.* Oxford: Oxford University Press.

International Monetary Fund. 1996. "Partnership for Sustainable Global Growth, Interim Committee Declaration Washington." Accessed November 16, 2021. https://www.imf.org/external/np/exr/dec.pdf

JOHNSTON, Michael. 2002. *Good Governance: Rule of Law, Transparency, and Accountability.* Edited by UNESCO. Accessed November 17, 2021. https://etico.iiep.unesco.org/sites/ default/files/unpan010193.pdf.

JOSEPH, Sarah. 2001. "Democratic Good Governance: New Agenda for Change." *Economic and Political Weekly.*

—. 2001. "Democratic Good Governance: New Agenda for Change." *Economic and Political Weekly*, 1011-1014. Accessed November 16, 2021. https://www.jstor.org/ stable/4410424

KANTAR. 2021. *Standard Eurobarometer 95. the EU and the coronavirus pandemic.* European Commission. Accessed November 20, 2021. doi:10.2775/401085.

KILLION, David. 2014. "Importance of good governance to comprehensive security." *OSCE Japan Conference on Sharing Experiences and Lessons Learned between the OSCE and Asian Partners for Cooperation in Order to Create a Safer, More Interconnected and World in the Face of Emerging Challenges.* 16 June. Accessed November 17, 2021. .csce.gov/international-impact/press-and-media/speeches/importance-good-governance-comprehensive-security

MOBARAK, Ahmed M. 2005. "Democracy, Volatility, and Economic Development", în , Vol. 82, No. 2, 2005, pp. 348–361." *The Review of Economics and Statistics*, 348-361.

OECD. 2012. "OECD Strategy on Development." Accessed November 17, 2021. https://www.oecd.org/development/oecd-strategy-on-development.htm

OKAFOR, Godson O., and Chinonye F. Malizu. 2014. "Exploring the synergy of democracy and national security for good governance in Nigeria." *IOSD Jurnal of Humanities and Social Science* 19 (1): 21-28.

PRZEWORSKI, Adam, Michael Alvarez, Jose Antonio Cheibub, and Fernando Limongi. 2000. *Democracy and Development: Political Institutions and Material Well-Being in the World, 1950–1990.* Cambridge: Cambridge University Press.

QUILES, Marco Just. 2013. *Is Good Governance good for Development? Impressions from the latest UN- 'Piont - Counter Piont'- Discussion Forum.* Accessed November 20, 2021. https://publicadministration.un.org/paconnect/Blogs/ID/25/Is-Good-Governance-good-for-Development-Impressions-from-the-latest-UN-Piont--Counter-Piont-Discussion-Forum

ROSE, Richard, and Caryn Peiffer. 2019. *Bad Governance and Corruption.* Cham: Palgrave Macmillan.

SKLAR, Richard L. 1987. "Developmental Democracy." *Comparative Studies in Society and History*, 686-714.

STOCKEMER, Daniel. 2009. "Does democracy lead to good governance? The question applied to Africa and Latin America." *Global Change, Peace & Security*, 241-255. Accessed November 16, 2021. doi:10.1080/14781150902872141.

The Robert Schuman Centre for Advanced Studies, Global Trade Alert, and The World Bank Group. 2020. "The Covid-19 Pandemic: 21st Century Approaches to Tracking Trade Policy Responses in Real-Time." Accessed November 23, 2021. https://www.globaltradealert.org/reports/54

The World Bank. 1994. *Governance. The World Bank's Experience.* Washington D.C.: The World Bank.

Woo-Cumings (Ed.), Meredith. 1999. *The Developmental State.* Ithaca: Cornell University Press.

DOI: 10.53477/2668-6511-22-03

THE MATHEMATICAL MODELING OF THE EPIDEMIC DISEASES INDUCED BY BIOLOGICAL ATTACK WITH CONTAGIOUS AGENTS

Viorel ORDEANU, Ph.D.,
Col. (ret.) Prof. MD SR, "Titu Maiorescu" University, Bucharest, Romania.
E-mail: ordeanu_viorel@yahoo.com

Lucia Elena IONESCU, Ph.D.,
"Cantacuzino" National Military Medical Institute for Research-Development, Bucharest, Romania. E-mail: ionescu.lucia@gmail.com

Abstract: *The current security context illustrated by the COVID-19 pandemic shows us that we have vulnerabilities, that there are threats and that there will be risks, including biological ones. In the field of BIO defense it is almost impossible to experiment at the general level. This can only be done on time in the laboratory, in vitro, in vivo and possibly in silico. The calculation methodology for the effects of possible attack with contagious biological warfare agents has certain assumptions and limitations. Considering that the population is homogeneous it results that the isolated groups, to which the infection it does not spread, will show an overestimation. Possible individual variations, particular diseases and asymptomatic cases are not taken into account so either an underestimation or an overestimation occurs. In the mathematical modeling of the epidemic diseases induced by biological attack with contagious agents can use the SEIRP model: Susceptible, Exposed and Infected, Infectious, Removed and Prophylaxis Efficacious Model. The study is important for medical operational planning.*

Keywords: *biological attack; living biological warfare agents; contagious agents; mathematical modeling; probable health losses.*

Introduction

Biological weapons are also called *the atomic weapon of the poor* due to the possible devastating effect of the attack, through health losses, psychological effect and countermeasures expenditures. To estimate the effect, the probable health losses must be calculated, by mathematical modeling of the epidemic induced by the biological attack with contagious agents. The principles of mathematical epidemiology have been adapted and are also presented in NATO documents, for unitary application in the allied armies.

The calculation methodology for the effects of the attack with contagious biological warfare (WBA) has certain assumptions and limitations for the calculation in cases on contagious agents. The population is considered to be relatively large and unstructured (homogeneous) for a regional or metropolitan epidemic and cannot be extrapolated to geographically separate military units. Considering that the population is homogeneous, it results that in the isolated groups, in which the contagion does not spread, an overestimation appears. For simplicity, possible individual variations, particular diseases and asymptomatic cases are not taken into account, so either an underestimation or an overestimation occurs. This assumption is justified by the complexity of the parameters in infectious diseases, which involve a biunivocal relationship between the pathogen and the host organism, each being influenced by natural and artificial environmental factors.

The population is considered to be relatively large and unstructured (inhomogeneous) for a regional or metropolitan epidemic and cannot be extrapolated to geographically separate military units. Considering that the population is homogeneous, it results that in the isolated groups, in which the contagion does not spread, an overestimation appears. For simplicity, possible individual variations, particular diseases and asymptomatic cases are not taken into account, so either an underestimation or an overestimation occurs. This assumption is justified by the complexity of the parameters in infectious diseases, which involve a biunivocal relationship between the pathogen and the host organism, each being influenced by natural and artificial environmental factors. The prediction errors in the current Covid-19 pandemic are illustrative in this regard.

For the situation of prophylaxis (by vaccination) or pre-exposure or intra-exposure prophylaxis (with individual and/or collective protective equipment) or post-exposure (with antibiotics or antivirals) the equation differs according to the SEIRP model: susceptible, exposed, infected, outgoing (discharged or deceased) and effective prophylaxis.

The human response to contagious agents incorporates the same set of mathematical submodules as to noncontagious agents: latency (incubation), mortality, disease duration, and disease severity over time (dynamics). These are incorporated in the SEIRP epidemiological model which includes: specificity (agent and disease), susceptibility (population), number of exposed and infected, infection (number of patients), „removed" namely exited (cured or dead), prophylaxis efficiency, to which are added the specific factors: the rate of transmission (R factor) and the spread of the contagious disease in the respective population. The dynamics of the epidemic can be presented schematically in the form of an algorithm with cohorts (groups) with evolution over time, from the exposed population to the cured and dead, adapted after Allied Medical Publication-8(C), (AmedP-8(C)), 11-38.

1. Model of calculation

The model (for example, US Army SEIRP) uses a set of equations that are solved sequentially daily for each time period (t) greater than or equal to 1 day (t = 1), the resulting cohorts being time dependent. The calculation for contagious does not estimate the medical treatment, the number of patients who are saved or the time required, so no specific time is provided for leaving the medical system (it is considered that the survivors remain indefinitely under medical care). This interpretation is medically useful only for certain cases with prolonged evolution, but it is a reality for military actions because it cannot be counted on those soldiers that they can continue the mission, so they will have to be replaced.

General formula is:

[17] $N0 = P(t) + S(t) + E(t) + I1(t) + I2(t) + R(t)$, where:

N0 = estimated total number of contagious patients
P(t) = estimated number of prophylaxis
S(t) = estimated number of susceptible ill people
E(t) = estimated number of exposed people
I1(t) = estimated number of stage 1 contagious patients
I2(t) = estimated number of stage 2 contagious patients
R(t) = estimated number of exited (cured or dead)

The equations embedded in the SEIRP methodology use a set of parameters as input data:

ά = probabilitaty that people with stage 1 disease will infect susceptible people
ρS = efficacy of prophylaxis in the susceptible cohort
ρE = efficacy of prophylaxis in the exposed and infected cohort
μE = period of time when individuals were in the cohort of exposed and infected
μ1 = period of time when individuals were in the cohort of stage 1 contagious patients
μ2 = period of time when individuals were in the cohort of stage 2 contagious patients
β(t) = rate of disease transmission over time

υon(t) = binary prophylaxis parameter (if prophylaxis was applied: Yes = 1 şi No = 0)
υoff(t) = binary prophylaxis parameter (if prophylaxis is discontinuous: discontinuous = 1 and continuous = 0)
pf(dn) = the probability of death, which in infectious agents is dose-independent, therefore:

[18] pf(dn) = pf

The initial number for which prophylaxis is effective in group n, if all individuals in have received prophylaxis, is:

[19] Pn(0) = în × ρ, where:

Pn(0) = the initial number of individuals in the group in whom prophylaxis is effective.

The infectivity submodel is calculated only if the prophylaxis is not effective, so the initial number of exposed, infected and patients in stage 1:

[20] En(0) = E1n(0) = (in × (1 – ρ) × PE(dn), where:

En(0) = initial number of exposed and infected people in group n
E1n(0) = the initial number of exposed and infected stage 1 patients in group n

The total number of individuals in whom prophylaxis is effective P(0) and the total number of individuals who have been exposed and infected E(0) is the sum of those in each group:

[21] $P(0) = \sum_{n=1}^{N} Pn(0) = \rho \sum_{n=1}^{N} In$

[22] $E(0) = \sum_{n-1}^{N} E1n(0) = (1 - \rho) \sum_{n-1}^{N} (in \times PE(dn))$

P(0) and E(0) values are input data for SEIRP. The individual progression for exposed and infected and patients stage 1 (E1n) to stage 2 (E2n) after the minimum incubation period is: E2n(0) = 0. We assume that initially there were no patients or evacuees, meaning I1(0) = 0 and I2(0) = 0 and R(0) = 0, the susceptible population is:

[23] S(0) = N0 – P(0) – E(0)

If each of these parameters is known, the equation is solved sequentially. The calculation stops at time t = the day when the transmission factor tends to zero, plus the time of manifestation of the disease, meaning:

[24] μE1 + μE2 + μ1 + μ2

Number of people for whom the prophylaxis is efficient:

[25] P(t) = P(t-1) + ρS × υon(t-1) ×S(t-1) + ρE × υon(t-1) ×E(t-1) - υoff(t-1) ×P(t-1)

Number of susceptible people in t moment:

[26] $\underline{S(t) = S(t-1) - \beta(t-1) \times S(t-1) \times [\acute{a} \times I1(t-1) + (1- \acute{a}) \times I2(t-1)] \Delta t}$
$N0 - \rho S \times \upsilon on(t-1) \times S(t-1) + \upsilon off(t-1) \times P(t-1)$

Number of exposed and infected people in a given moment:

[27] E(t) = E1(t) + E2(t)

From whom in stage 1, for time t ≤ minimum time of incubation:

[28] E1(t) = E1(t-1)

And for time t > minimum time of incubation:

[29] $\underline{E1(t) = E1(t-1) + \beta(t-1) \times S(t-1) \times [\acute{a} \times I1(t-1) + (1- \acute{a}) \times I2(t-1)] \Delta t}$
$N0 - \beta e \times \upsilon on(t-1) \times E1(t-1) - E1(t-1) \Delta t / \mu E$

For the calculation of the number of exposed and infected stage 2, the minimum incubation time, t min, is also considered:

[30] for t < tmin E2(t) = 0

[31] for t = tmin E2(t) = E1(t-1)

[32] for t > tmin $\underline{E2(t) = E2(t-1) + E2(t-1) \Delta t}$
$\mu E1 - E2(t-1) \Delta t / \mu E2$

For the number of patients in stage 1 at time t:

[33] $$I1(t) = I1(t-1) + \frac{E2(t-1)\,\Delta t}{\mu E2 - I1(t-1) / \mu 1}$$

and for the number of patients in stage 2 at time t:

[34] $$I2(t) = I2(t-1) + \frac{I1(t-1)\,\Delta t}{\mu 1 - I2(t-1)\,\Delta t / \mu 2}$$

Number of exited people (cured or deceased) at time t:

[35] $$R(t) = R(t-1) + I2(t-1)\,\Delta t / \mu 2$$

Number of deaths:

[36] $$Rf(t) = pf \times R(t)$$

Number of patients remaining in the medical system:

[37] $$Rm(t) = R(t) - Rf(t)$$

The methodology for calculating the human response to contagious agents is supplemented by the calculation for new cases and new deaths. The estimation of diseases with contagious biological agents, at a given moment, is calculated on cohorts: population at risk P(t), exposed E(t), patients stage 1 - I1(t), patients stage 2 - I2(t), hospitalized Rm(t), deaths Rf(t), number of new cases per day - I1 new(t) and I2 new(t), new deaths per day Rf new(t). The estimate of the number of wounded/sick in battle is calculated according to the level of severity of the disease at each stage and differs according to the biological agent/disease. It is calculated the total number and new cases per stage, namely WIA I1 new(t) and I2 new(t).

Number of new cases in stage 1 at time t:

[38] $$I1\ new(t) = E2(t-1)\,\Delta t / \mu 2$$

Number of new cases in stage 2 at time t:

[39] $$I2\ new(t) = I1(t-1)\,\Delta t / \mu 1$$ where:

I1 new(t) = number of infected people who become stage 1 in time period t, and I2 new(t) = number of infected people who get stage 2 disease in time period t.

Number of new deaths at time t:

[40] $$Rf\ new(t) = pf \times (I2(t-1)\,\Delta t / \mu 2$$ where:

Rf new(t) = number of dead people in the period of time t.

From these data we calculate WIA and DOW taking into consideration the time, after the incubation period, in the form of a specific algorithm, (AmedP-8(C)), after which we adapted estimation examples for health losses caused by the most contagious WBA likely to be used in an attack (Allied Medical Publication-8(C), 223-227).

2. Estimation of plague cases

Plague (pestis) is a very serious infectious-contagious disease caused by the cocobacillus *Yersinia pestis* that can cause ***bubonic plague*** (with lymph node infection), ***lung plague*** or both. The methodology considers only the aerosolization variant, because it is the most efficient from a military point of view, compared to the classic methods of vector distribution (sick rats or infected fleas). The disease can be treated with antibiotics both curatively and prophylactically after exposure. There is a vaccine for prophylaxis and if available it protects against disease or reduces the severity of the disease, but the lung form has a very high mortality. However, this vaccination incapacitates the military for hours or days. (Allied Medical Publication-8(C), 228)

Infectivity: the probability of plague disease is modeled by the log-probit function with 1 probit/log dose at the value of 20,000 CFU, but with very high variability. (Allied Medical Publication-8(C), 229-231)

The mathematical function of cumulative distribution is with lognormal distribution

[41] PE pestis (dn) = ½ + ½ {erf ($\frac{\ln(dn) - \mu}{\sigma\sqrt{2}}$)} where:

n = number of groups
PE pestis (dn) = number of people exposed to the dose of plague in group n who will get sick (exposed and infected)
Dn = pestis dose (UFC) in group n
μ = natural variable of logarithm of infectious dose 50%
ln (DI50) = in (66 UFC) = 4.1897
m = probit (1 probit/log dose) l/m $1/1$
σ = standard deviation of natural logarithm variable $e =$ e = 2.7193
erf = error of function

$$erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t2} dt$$

Lethality is considered in untreated pneumonic plague to be practically 100%, so the probability of death is: pf = 1.

Recommended parameters for plague epidemiology according to AMedP-8(C) table A47:
μE1 = 1 day
μE2 = 3.3 days
μ1 = 1 day in stage 1, with severity level 2
μ2 = 1.5 days in stage 2, with severity level 4
Δt = 1 day
ά = 0
P = N/A (variable)
PS = 0.95
PE = 0.95
υon(t) = 1 for t = 0 days and 0 for 1 ≠ 0 days
υoff(t) = 1 for t = 7 days and 0 for 1 ≠ 7 days

Secondary (β) ***transmission rate*** of plague according to historical epidemics: days 1 and 2 transmission 0, days 3-17 high transmission, days 18-32 low transmission, day 33 very low and after 33 days = 0. From this model transmission started the quarantine isolation method (quaranta - 40 days in Italian) during the plague pandemic.

Model parameters for estimating plague cases. Infectivity and lethality sub-models in plague patients are incorporated into the SEIRP model. The disease profile is unique to non-survivors, with a period of symptoms characteristic of lung infection and two stages of the disease, so there is no other disease profile because mortality is 100%. Disease profile for deceased plague patients is shown in Table 1, adapted from AmedP-8(C), 234.

Table no.1: Disease profile for plague deaths

Criteria	Stage 1	Stage 2
Signs and symptoms	Fever Headache Nausea Vomiting Vertigo Tachypnea	Fever Dyspnoea Dry cough that becomes productive Bloody sputum Cyanosis Illness

Criteria	Stage 1	Stage 2
	Tachycardia Dry cough	Delirium Ataxia Confusion Disorientation Apathy Coma Collapse Respiratory arrest
Severity	2 (moderate)	4 (very severe)
Treatment	If untreated it goes to stage 2, if the right treatment is started it can stop going to stage 2	Even if treatment is started, the patient dies

It should be noted that throughout history, plague epidemics have been the most lethal infectious diseases.

Antibiotic prophylaxis is recommended immediately after exposure to pestis aerosols, ciprofloxacin, other fluoroquinolones or other oral antibiotics or within a maximum of 24 hours and may reduce mortality by 95%. Treatment can also be done with injectable Streptomycin for 10 days (AmedP-8(C), 236).

3. Estimation of smallpox cases

Smallpox is a serious viral disease with high mortality but preventable by vaccination. In 1980 it was declared by the WHO as eradicated, being the first infectious-contagious disease to disappear as a result of modern medicine. Since then, there has been no vaccine and no smallpox vaccination. If an aggressor uses smallpox virus for biological attack, the consequences could be catastrophic because the younger generations are not vaccinated and the resumption of vaccine production takes a long time. The virus spreads through the air and through contact, causes specific damage to the skin and mucous membranes and if inhaled destroys the lungs and the disease is fatal.

Smallpox parameters. Infectivity is 100% but the disease is triggered only if the dose is sufficient, over 10 UFP (units forming plates), otherwise the probability of infection is 0.

PE smallpox (dn) = 1 for dn $\geq$ 10 UFP and

PE smallpox (dn) = 0 for dn $<$ 10 UFP

Lethality is dependent on immunity, respectively on vaccine status: 30% in unvaccinated and 3% in vaccinated prophylactically or immediately after exposure, the others exposed and infected will get the disease and be cured he model parameters for the evolution of smallpox cases are presented in Tables 2 and 3 (adaptation according to AmedP-8(C). (Allied Medical Publication-8(C), 240).

Table no. 2: Smallpox model parameters for comparing survivors/non-survivors, with and without vaccination

Parameter	Survivors	Non-survivors
μE1	7 days	7 days
μE2	4.6 days	4.6 days
μ1	2.8 days(stage 1, severity level 2)	2,8 days (stage 1, severity level 2)

Parameter	Survivors	Non-survivors
μ2	12.6 days (stage 2, severity level 3)	12.6 days (stage 2, severity level 4)
μ3	4 days (stage 3, severity level 1)	N/A!
Δt	1 day	1 day
ά	0	0
P	0.95 / N/A	0.95 / N/A
PS	N/A / 0,95	N/A / 0.95
PE	N/A / 0,85	N/A / 0.85
υon(t)	N/A / 1 for t = 1 day and 0 pentru t > 1 day	N/A / 1 for t = 1 day and 0 for t > 1 day
υoff(t)	N/A / 0	N/A / 0

Secondary transmission of smallpox, according to historical epidemiological data, mainly after the smallpox epidemic in the former Yugoslavia in 1972, shows a specific evolution. In the first 8 days it is not transmitted, in days 9-11 the transmission is moderate, in days 12-20 it is high, it decreases in days 21-28, then it increases again in days 29-37, it returns to moderate transmission in days 38- 59, and from day 60 it is no longer transmitted.

The smallpox virus is no longer in nature, the disease has been eradicated for four decades, so a smallpox attack would be incriminating for the aggressor. The only officially and legally stored strains of smallpox virus are in the United States, Russia and the United Kingdom, but there may be others illegally kept by states or non-state organizations. The consequences of the biological attack with smallpox depend on the parameters of the presented submodels. The profile of the disease is different for surviving and non-surviving smallpox patients. For survivors the symptomatic period is divided into 3 stages, and for non-survivors into 2 stages with different signs and symptoms. The usual smallpox profile is shown in Table 9, comparing for survivors and non-survivors (Allied Medical Publication-8(C), 248).

Table no. 3: Comparison of the evolution of smallpox patients

Signs and symptoms	Survivors	Non-survivors
Stage 1 Severitay level 2 (moderate), evolution to stage 2	Fever 38-40.5˚C Illness Vomiting Chills Headache Back pain Abdominal pain Raving	Fever 38-40.5˚C Illness Vomiting Chills Headache Back pain Abdominal pain Raving
Stage 2 Severity level 3 (severe) evolution to stage 3 (if survives)	Fluctuating fever (decreases but with peaks at 40˚C) Sore throat, dysphagia Exantem pharyngeal Maculo-papular rash on the face, mouth, pharynx, hands, forearms Maculo-papular rash on the lower limbs After a few days: Blisters that turn into pustules	Fluctuating fever (decreases but with peaks at 40˚C) Sore throat, dysphagia Exantem pharyngeal Maculo-papular rash on the face, mouth, pharynx, hands, forearms Maculo-papular rash on the lower limbs After a few days: Blisters that turn into pustules, leave scars Severe toxemia, with multiple organ failure Death
Stage 3 Individual will likely recover from illness	The general condition is improving The pustules form crusts, which when removed leave depigmented depressions after healing	

Scenario characterization: attack with aerosols with biological cloud with very high concentration (approx. 1 million PFU/min/m^3) in the central area and peripheral decrease, and after passing the cloud the concentration tends to zero. The model is valid for any other lethal virus with high contagiousness: Ebola, Marburg, influenza, coronaviruses (SARS, MERS, SARS-CoV-2) etc.

The exposure medium is considered for accumulation for 10 min, and the dose is influenced by local factors, inhalation (respiration rate = volume of inhaled air per minute) depending on the activity (physical effort). Shelter in buildings or vehicles reduces the absorbed dose (SF vent μ) depending on ventilation.

Physical protection (PFn) consists of personal CBRN protective equipment (mainly gas mask) and collective protection in buildings or vehicles equipped with filter ventilation. US Army standards provide a protection factor of 1/1667 for masks and 1/3000 for filter ventilation systems, which should provide very good protection against CBR agents. The calculation of the dose must take into account all these factors, and the calculation of prophylaxis and infectivity, in groups, takes into account pre-exposure prophylaxis by vaccination.

The example shown with smallpox virus does not present the most dangerous situation because there is an effective smallpox vaccine, which the Cantacuzino Institute also manufactured industrially before the cessation of production and if necessary could have resumed its manufacture. But for other contagious viruses, possibly to be used as biological weapons, there are still no vaccines: hemorrhagic fevers, encephalitic fevers, etc. It turns out that the effect of the attack would be very high (very good cost/benefit ratio) but also the risk of pandemic would be so high that the medical risk/benefit implications would be at an unacceptable level. The current COVID-19 epidemic/pandemic is like an unwanted *situational experiment*, in which we are confronted with a biological agent only partially known and against which we are still experiencing specific medical countermeasures (Viorel ORDEANU, Lucia Elena IONESCU, 2020, 48-61).

4. Limitations of mathematical modelling in epidemiology

Contagious viral biological agents are extremely dangerous because antiviral drugs are less effective than antibiotics in bacterial agents, and for many viruses there is no recommended treatment, namely etiological and specific. This does not mean that the respective patients will not be treated, but all appropriate pharmacological and non-pharmacological means will be applied as a non-specific treatment: symptomatic, adjuvant, complementary, *off label*, etc. to try to heal the patient. Contagious biological agents have the highest degree of efficiency in biological warfare but also an unacceptable level of risk. The only logical solution is the real and definitive renunciation of biological weapons/agents and the exact application of the provisions of the Geneva Convention on the Prohibition of Biological and Toxin Weapons, 1972, (URL: https://www.un.org/disarmament/biological-weapons).

The classic model for contagious bacteria is plague, a zooanthroponotic disease known since Antiquity, which has caused the deadliest known natural epidemics and pandemics in history, but today many countries have vaccine and antibiotic therapy. According to the plague model, the effects of other contagious bacterial diseases can be calculated, usable for biological attacks.

The model for contagious viruses is smallpox, a human-specific disease also known in Antiquity, which in endemic and epidemic form has also caused many deaths, but has been eradicated including by mass vaccination for almost two centuries. The smallpox model can be applied to any other contagious viral agent, but we do not have the recommended vaccine and/or treatment for all of them. It follows that the serious situation presented in this example could be even worse if those viral agents are used. A much worse situation would be if hybrid viruses

(for example, Ebola-smallpox) or new synthesized viruses in the laboratory are used, about which almost nothing is known. It is necessary to completely abandon the biological agents of war and bioterrorism, first of all the contagious ones that can be a major danger to humanity.

The calculation examples presented for the effect of the attack with contagious biological agents are extracted and adapted from the NATO specialized literature, for the use of military planners (medical and non-medical) in the situation of biological warfare. They seem very scientific, are based on historical medical experience and are processed with appropriate mathematical formulas. But the reality shown by the current Covid-19 pandemic, seen as a *situational experiment,* shows that everything is relative and the value of the estimates is only indicative, the theory does not always match the practice.

The Covid-19 pandemic has led to a huge number of new works, which double every two weeks. Many of these papers are first published on *preprint* servers without undergoing the *peer review* process, which raises questions about the quality of many of them. This multitude of scientific and pseudo-scientific information *compromises the mathematical modeling of the epidemic,* and the medical and non-medical countermeasures are chaotic and ineffective, as can be seen in the evolution of the current pandemic. A *start-up* company says its platform - called Scite.ai - can automatically inform readers if the work has been supported or contradicted by scientific research. By May 2020, the platform had analyzed over 16 million full-text scientific articles from publishers such as BMJ Publishing Group in London and Karger in Basle, Switzerland. However, Jodi Schneider, from the University of Illinois at Urbana-Champaign, says the platform has its limitations related to the literature it has access to and machine learning algorithms. At this time, the *Scite.ai* analysis of the Covid-19 database is not fully automated, so there is sometimes a delay in how quickly *preprints* are analyzed by the tool. *Scite.ai* has about 1,000 visitors per day and approx. 2,700 registered users, the number has been increasing since the site started asking users to register to view the full citation analysis for a given paper (Roxanne Khamsi, 2020). Today, the number of citations of a paper is considered by researchers as a measure of its degree of influence. However, even if a paper is highly cited, it does not mean that it is a reference, says Elizabeth Suelzer, a librarian at the Medical College of Wisconsin Libraries in Milwaukee. For example, the famous study withdrawn in 1998 by former doctor Andrew Wakefield, who claimed that there is a link between autism and vaccines. It is extremely quoted, but most of these quotes are negative. In such situations a tool like Scite.ai could be very helpful.

Josh Nicholson, co-founder and CEO of *Scite.ai,* first recognized the need for such an instrument in 2012 during his doctorate in cell biology at Virginia Polytechnic Institute and Blacksburg State University when he read a commentary on *Nature* intensely disputed on scientific reproducibility. In it, a researcher at the biotechnology company Amgen in Thousand Oaks, California, revealed that scientists there could not reproduce the results of 47 of the 53 "reference" studies on cancer. This encouraged Nicholson and biologist Yuri Lazebnik to propose a new citation method to indicate whether a particular study or its findings were verified in subsequent reports. Thus, the two researchers launched Scite.ai in April 2020. The algorithm extracts the text of articles from partner publishers (for example, Rockefeller University Press in New York City and Wiley in Hoboken, New Jersey), and after analysis, eight out of ten papers reported by the tool as supporting or contradicting a study are relatively correctly classified, according to the founder. (Khamsi, Nature, 2020).

Following the same idea, computer simulation programs and algorithms for estimating the evolution of epidemics/pandemics such as Covid-19, are required to be made public to verify their reproducibility. The discussions are extremely heated because most of those who write such programs do not agree.

Epidemiologist Neil Ferguson, who led the simulation of the coronavirus pandemic at Imperial College London, presented basic estimates of the impact of the pandemic at a private meeting of the UK's leading emergency advisory group at a meeting on 27 February 2020. His figures showed estimates of half a million deaths if nothing is done to stop the virus and modeled how various political interventions could help. The politicized debate over this code demonstrates why scientists may still be reluctant to openly launch the code behind their work. Ferguson – who did not comment on the criticism at the time – agrees that the simulation did not use current methods of coding best practices because it had to be adapted from a model created more than a decade ago to simulate a flu pandemic. He said "There was no time to generate new simulations of the same complexity from scratch," he says, but the team used more modern coding approaches in its other work. However, "none of the criticisms of the code affect math or simulation science" (Chawla, Nature, 2020).

5. Experimentation *in silico* – constructive simulation

Experimentation using constructive simulation is a viable and efficient tool, but insufficiently known and used. At national level, this perspective was mentioned in the *Modeling and Simulation Strategy (M&S) in the Romanian Armed Forces,* for the period 2014 – 2024.

In the Military Strategy of Romania (2021), among the defense capabilities and the priorities of their realization is the development, at joint level, of the national military training capacity through simulation, but also the development of operational medical capabilities and strengthening the medical system of the Ministry of National Defense. (https://sg.mapn.ro/app/webroot/files/project/Strategia%20militara%20a%20Romaniei % 202.pdf)

The current security context (the Covid-19 pandemic) shows us that we have vulnerabilities, that there are threats and that there will be risks, including biological ones. We must be aware that it would be good to be able to counter them before they materialize, during and especially after, in order to liquidate the consequences.

However, the theoretical conception must be validated by practice. In the field of BIO defense it is almost impossible to experiment at a general level. This can only be done from case to case, in the laboratory, in *vitro*, in *vivo* and possibly in *silico*. Therefore, in the period 2013-2017, in the former *Medical-Military Scientific Research Center* (MMRC) institutionally taken over by the "Cantacuzino" Institute were conducted constructive simulation experiments in collaboration with the *Center for War Games and Doctrinal Experimentation* which were basic tools in a project of medical-military scientific research for the optimization and implementation of countermeasures of the bioterrorist attack with non-contagious biological agents, in accordance with NATO/EU standards and compatible with the capabilities of the Alliance.

These experiments are unique in the Romanian Armed Force, and the research results were used for the education and training of military personnel and students of the Medical-Military Institute.

The activity can be useful for for understanding and solving complex situations in the field of military medicine and CBRN protection, with the advantage that the benefits can be obtained at extremely low costs. It could also be used as a model for constructive simulation exercises for biological attack with contagious biological warfare agents.

Constructive simulation uses *Models and simulations* in which simulated people operate simulated systems and real people provide the inputs for this type of simulations, but are not involved in determining the outputs of the simulation process. (Viorel Ordeanu, Manuel DOGARU, Lucia Ionescu, 2015, 103-109).

The development process of the common synthetic operational environment, necessary for modeling and simulation, uses pre-built or built databases, generated by the dedicated software applications detailed in the exercise plans made by its director and the evaluating director. The results are useful for military and medical-military education as well as for estimating in advance the consequences of a biological attack.

Conclusions

Biological attack with contagious biological agents can be devastating both through the direct effect and through the infectious-contagious disease that can spread as an epidemic or pandemic and get out of control.

In the mathematical modeling of epidemic diseases induced by the biological attack with contagious agents, the SEIRP model can be used, the calculation methodology having however called assumptions and limitations.

The approach from this point of view is important for operational medical planning and for medical countermeasures, being an important element in the decision-making process regarding the planning of the operation.

BIBLIOGRAPHY:

***, Coronavirus in context: Scite.ai tracks positive and negative citations for COVID-19 literature, doi: https://doi.org/10.1038/d41586-020-01324-6)

***, Geneva Convention on the Prohibition of Biological and Toxin Weapons (BTWC 1972). (https://www.un.org/disarmament/biological-weapons).

CHAWLA, Dalmeet Singh. 2020. „Critiqued coronavirus simulation gets thumbs up from code-checking efforts". Nature. 08 June 2020. Accessed 29.09.2021. https://www.nature.com/articles/d41586-020-01685-y

https://sg.mapn.ro/app/webroot/files/project/Strategia%20militara%20a%20Romaniei%202.pdf

KHAMSI, Roxanne. 2020. „CORONAVIRUS in context: Scite.ai tracks positive and negative citations for COVID-19 literature". Nature. 01 May 2020. Accessed 29.09.2021. https://www.nature.com/articles/d41586-020-01324-6

ORDEANU, Viorel, IONESCU Lucia Elena. 2020. STRATEGIES XXI International Scientific Conference, The Complex and Dynamic Nature of the Security Environment, "The impact of the COVID-19 pandemic on national and international security".

ORDEANU, Viorel, DOGARU, Manuel, IONESCU Lucia. 2015. Buletinul Universităţii Naţionale de Apărare „Carol I". "Experimental informatical model for defence exercises against biological weapons and bioterrorism".

Technical Reference Manual: NATO Planning Guide for the Estimation of Chemical, Biological, Radiological, and Nuclear (CBRN) Casualties, Allied Medical Publication-8(C), (AmedP-8(C)), 11-38, 36

DOI: 10.53477/2668-6511-22-04

ESTIMATION OF PROBABLE HEALTH LOSSES IN BIOLOGICAL ATTACK WITH NON-CONTAGIOUS AGENTS, BY MATHEMATICAL EPIDEMIOLOGY

Viorel ORDEANU, Ph.D.,
Col. (ret.) Prof. MD SR, "Titu Maiorescu" University, Bucharest, Romania.
E-mail: ordeanuviorel@yahoo.com

Lucia Elena IONESCU, Ph.D.,
"Cantacuzino" National Military Medical Institute for Research-Development, Bucharest, Romania. E-mail: ionescu.lucia@gmail.com

Abstract: *In the case of attack with CBRN Weapons of Mass Destruction, the use of* biological warfare agents *is likely to amplify the effect on the living force, in order to infect, lethal or non-lethal, as many enemy as possible. The military medical service must be able to prevent, diagnose, treat and recover all affected military and the civilian population in the area. Health losses must be recovered in their entirety. Mathematical modeling of the epidemic induced by biological attack is useful for planning the forces and means of the military medical service, for medical planning the offensive or defensive operation, logistics and human resources needed for medical support and replacement. The estimates resulting from the calculations according to the formulas recommended in the specific NATO documents allow the optimization of the medical and non-medical countermeasures for the liquidation of the consequences of the biological attack.*

Keywords: *biological attack; probable health losses; biological warfare agents; mathematical modeling; medical operational planning.*

Introduction

Biological attack is a reality of the contemporary world. The use of living pathogens has been used since Antiquity for the disease of humans, animals and/or plants, with certain specific objectives. But an intentionally provoked epidemic is likely to spread, get out of control and become a pandemic or create a biological crisis. Biological warfare agents (BWA) are classified into living agents (bacterium and viruses) and non-living agents (toxins) and are listed in the North Atlantic Treaty Organization (NATO) documents STANAG Med and CBRN.

For effective countermeasures it is necessary to estimate as accurately as possible, by mathematical epidemiological calculations, health losses (contaminated, infected, sick people) and total losses (deaths) to quantify the epidemic, in order to prepare the necessary forces and means and eliminate the consequences of biological attack, by medical and non-medical countermeasures.

Specific NATO terms are: "WIA" (wounded in action), namely injured in battle, "KIA" (killed in action), namely dead in battle, "DOW" (died of wound) meaning dead later due to injury or illness in battle, as opposed to the dead and wounded by accidents or the ordinary sick people.

1. Health losses

Due to the particular conditions in the theater of operations (TO) in case of a biological attack, effects could appear on the military, their fighting and work capacity could be reduced and it is possible that the health losses are registered: sick, wounded, shipwrecked, intoxicated, irradiated, stressed, etc. who can no longer fulfill their mission.

The medical service must be able to prevent, diagnose, treat and recover all soldiers in this situation, and as far as possible for the civilian population in the area. Health losses must be recovered almost entirely for combat, for work or at least for life. ***The total human losses*** are represented in addition by: dead, missing, prisoners, etc.

The severity of diseases and injuries is in principle classified into six severity levels according with North Atlantic Treaty Organization (NATO) Planning Guide for the Estimation of CBRN Casualties- AMedP-8(C) (2010):

1. Severity level 0 (no observable effect) = unobservable effects, asymptomatic, although the person has been exposed to harmfull emission (agent, effect), is contaminated or even infected, but shows no symptoms; the military continues his mission;

2. Severity level 1 (Mild) = the patient has (objective) signs and (subjective) symptoms but can take care of himself (self-said) or unqualified people (mutual aid) on the spot or at the injured meeting point and can continue his mission;

3. Severity level 2 (Moderate) = shows obvious signs and symptoms, which require first aid (paramedics) at the medical point of the unit, sometimes requires medical evacuation and sometimes the mission cannot be continued;

4. Severity level 3 (Severe) = shows signs and symptoms that endanger his life, an acute illness that requires hospitalization ROL 1 (qualified medical aid), the treatment may cure him or not; the military cannot continue the mission;

5. Severity level 4 (Very severe) = the signs and symptoms are very serious, the person would not survive in the absence of specific medical care in the hospital ROL 2 (specialized medical aid), the soldier is in danger of death; he cannot continue his mission;

6. Severity level 5 (Extreme severe) = includes severely wounded or sick, who will be evacuated to ROL 3 hospital or dying soldiers, who are no longer considered for battle planning and are managed according to NATO AMedP-8(C).

Depending on the situation, the medical evacuation will be done "by itself" (with own means) or "to itself" (with specialized MedEvac means) in successive stages or directly on destinations (medical competencies), if necessary with means of road transport, railway, naval, air or by any other means. The injured and the sick who present an emergency will have on them, in a visible place, a standard medical file that also specifies the emergency category, with a color code.

Health losses are numerically in the form of a pyramid: most people are healthy or seemingly healthy and form the basis of the pyramid, then we have the 6 levels, descending, and the top of the pyramid is represented by the wounded/deceased patients.

It is generally considered that losses below 10% do not significantly reduce combat capability (the principle of the Romanian Armed Forces of "decimating" troops fleeing the battlefield). But losses, both of health nature and total, affecting more than half of the troops require the immediate replacement of the entire unit and withdrawal to a recovery area. The Romanian Armed Forces had this situation twice at the operational level, due to the cholera epidemics: in Balkan War II and in the World War I. These were medically solved by the teams of prof.dr. Ioan Cantacuzino using as means cholera vaccination, quarantine, and other medical measures. (Ordeanu Viorel, 2021).

It should be noted that the evolution of an epidemic and the health losses it causes are somewhat similar to troops and the civilian population, or to natural epidemics or those caused by biological attack. But the results are variable for public health depending on the pathogen, dissemination, receptivity of the population, the effectiveness of individual and collective protection, treatment and health logistics.

The biological attack

The existing conditions in TO favor the appearance of infectious-contagious diseases and epidemics. In all wars there were more sick people than wounded and more died of infectious diseases than dead in battle, including in the World War I. But in World War II, almost all military health services applied adequate medical countermeasures and there were no major epidemics, except those caused intentionally. The intentional illness of the enemy with infectious-contagious diseases has been known for a long time, even before the discovery of microbes. Currently, "biological warfare" is well-founded for offensive and defensive, tactical, operational and strategic purposes, with lethal or disabling effect, because it is the cheapest (calculated in dollars/victim) and destroys only the living force, leaving weapons and technique in working condition. (Ordeanu V., Andries A.A., Hincu. 2008; Ordeanu, V., Necsulescu. M., Ionescu, L.E., Popescu, D.M., Bicheru, S.N., Dumitrescu, G.V., Hertzog, R.G. 2008)

The intentional spread of living pathogens can be catastrophic in time of war, and disease and death affect troops and the civilian population. But they can also spread to the person who triggered the biological attack, and if they get out of control, a pandemic can occur. This was also the main reason why biological attack was banned by the Geneva Convention (BTWC 1972). (https://www.un.org/disarmament/biological-weapons). But the methods and techniques of biological warfare have been taken over by terrorist organizations for actions of bioterrorism and biocrime. In the case of natural infectious-contagious biological agents or BWA, there is the same risk of mass spread, out-of-control, biological crisis and finally pandemic, as the natural COVID-19 epidemic is now underway. As a result, international law prohibits any research into offensive biological weapons and/or living or non-living biological agents capable of causing mass disease. But it is believed that the Great Powers, which have nuclear weapons (permitted by international law) could use the other WMD (prohibited by international law) because they can not be prevented from doing so. (Ordeanu V. & colab. 2012, 978-973).

Biological casualty is any person who becomes ill, is injured or dies as a result of exposure to biological agents or combined injuries. The biological attack is more insidious than other chemical, biological, radiological and nuclear (CBRN) weapons of mass destruction (WMD) attacks due to the extremely small amounts of infectious or toxic material affecting personnel. Unlike chemical warfare agents (CWAs), the infectious cloud is invisible, colorless, odorless, tasteless, does not alert organoleptically, and instrumental detection is late and nonspecific (regardless of what is written in the manufacturer's leaflet). The comparison of the dose of exposure to CWA and BWA is presented in table no. 1. The infectious doses are presented in table no. 1 (adaptation after AMedP-8(C)).

Table no. 1: Comparison of exposure factor EFn, t

Activity level	**CWA**	**BWA**
Light	1	15 liters of air/min
Moderate	2	30 liters of air/min
Heavy	5	75 liter of air/min

The methods of estimating the victims of WMD CBRN attacks are different depending on the agent(s) involved and the scenario, but are based on NATO recommendations. From a medical-military point of view, the typical situation is applied at the level of a Large Operational Unit, for example the Infantry Brigade, with different scenarios, depending on the tactical, operative or strategic situation. The NATO AMedP-8(C) Manual presents calculations for 11 CBRN agents: 3 CWA, 3 RWA and 5 BWA, most likely to be used as a model for other agents with similar behavior. Calculation methods for individual dose, dosage, magnitude of damage after exposure to CBRN agents, etc. are described.

The application of the methodology offers the ability to estimate the number of victims over time (dynamics per day): before the disease manifests itself, the incubation period, the incidence of injuries and the degree of severity. The results help military planners, staff officers, medical service, logisticians and commanders to allocate and/or demand adequate quantity and quality forces and means, transport of patients, evacuation of formations, supply and replenishment of stocks of sanitary-pharmaceutical and logistical materials, as well as facilities for decontamination of patients, triage, treatment, specific hospitalization, etc.

The methodology is primarily needed for planning, but can also be useful for real situations if it is based on real-time reported data. But, like any probabilistic calculation, it does not apply to individual cases for diagnosis, prophylaxis and/or treatment. Each epidemiological event has its own unique features and a dynamic multifactorial evolution that is difficult to predict. In the future, it would be possible to estimate through Artificial Intelligence (AI) programs based on previous experience and on modeling the current evolution.

From a medical-military point of view, *aerosol dispersion attack* (the most effective WBA dissemination technique) with anthrax spores or toxins, although causing mass epidemic diseases, is not considered contagious, unlike the other listed WBAs.

This methodology also includes the information needed to estimate the acute human response to non-contagious WBAs and their effects. It is obvious that the set of parameters cannot be exhaustive, and if other WBAs or any other pathogenic biological agents are used concomitantly or successively in association, or in ***combined attacks*** with WCA and/or WRA etc. the disease can be significantly potentiated.

In order to be applied, the methodology must somewhat simplify the reality, so it does not take into account the combined attacks, opportunistic infections, overlap with natural epidemics, living conditions, mental stress and other factors that influence the infectious disease. There are not taken into account: civilians of any kind, detainees, prisoners and missing persons, but only the personnel of the respective unit, and all the others are "collateral losses". Due to the particular complexity of the effects of biological attack, the examples are limited to biological attack scenarios with bacterium (in vegetative or sporulated form), with viruses or toxins, by aerosolization on a large operational unit with its units and subunits, with the military spread in different locations (*icon*).

The declaration as sick, injured or dead people is made according to the criteria established by the NATO, which concerns victims, as follows:

a) Military killed in mission = KIA or *prompt fatality* or *killed individual in action*;

b) Military wounded in combat = WIA or *wounded individual in action*, includes all types of injuries: penetrating and non-penetrating wounds, contusions, fractures, burns, crushing, infectious diseases, intoxications, asphyxiation, irradiation and any effects of conventional or unconventional weapons or CBRN agents;

c) Military wounded or sick deceased = DOW or *died of wounds*, delayed fatality meaning any death of a victim who dies as a result of a wound or disease acquired in battle. (NATO AMed-8(C), 4).

The methodology does not take into account the change in time of the severity level of the disease (evolution). The main input data for the application of the methodology are:

1. Estimating the CBRN environment, agent or effect present in the physical environment in which the military interacts during the attack; it is based on external information sources: CBRN defense subunits, medical teams, CBRN risk prediction models, etc.

2. Development of the scenario, the geographical position of the military according to time, individual physical protection (mask, equipment) and/or collective (vehicles, buildings, shelters) and physiological factors (physical effort, respiratory flow, etc.).

The scenario requires the characterization of the CBRN environment, the initial exposure, the amount of agent and the effects associated with each subunit, the time and severity of the disease in dynamics. For biological agents, the human response to exposure is estimated, separately for contagious and non-contagious agents, in order to estimate the subsequent evolution of diseases.

The methodology estimates the victims (health losses) according to four main **parameters**:

1. ***Population at risk*** (PAR), respectively the number of soldiers actually exposed;

2. ***The disease rate***, namely the percentage expression in the PAR of the new KIA, WIA and DOW cases;

3. ***The profile of the disease,*** which shows how many new cases evolve over time;

4. ***The flow of victims*** characterizes the change in the classification of patients (for example from WIA to DOW).

2. Limitations of applying mathematical methodology

The limitations depend on the input data, the level of uncertainty, the overestimation or underestimation of the effects, and the degree of impact of the approximations is unknown. The additional errors are attenuated by the minus errors and the result is close to the average of the real values, so the estimation presents a reasonable relativity.

The methodology assumes that all soldiers have a good state of health, without pre-existing diseases or poor physiological conditions or other factors that increase susceptibility to alter the body's response or contribute to potentiating risk factors, which would lead to underestimation of casualties. This methodology does not apply to civilians, because they are more susceptible to CBRN agents: they do not have special equipment, they do not have training, they do not have specialized medical assistance. For some CBRN agents, this methodology cannot serve as a model for medical countermeasures, but only for calculating the total losses that will reduce the unit's combat capability. A particular situation is presented by the post-exposure prophylaxis in the chemical attack: the use of the self-injection syringe (with atropine, oxime, etc.) temporarily reduces the fighting capacity of the military, but increases the survival. The methodology does not include medical treatment, so mortality is calculated in its absence, as a standard situation. It is considered if the sick are to be treated, the number of dead decreases and the number of sick increases. But it is not possible to estimate precisely who will get sick and how severe or if he will die, but only the total number of illnesses in the time interval. (NATO AMed-8(C), 8)

Neither the recovery of the patients in time for their return to battle is calculated, because the duration of the disease cannot be predicted accurately, nor the results of the treatment. It also does not take into account the psychological effects of battle stress that can affect some staff, which will need medical care.

Assumptions (initial presumptions) in using the methodology

The presented mathematical methodology assumes, in accordance with NATO doctrine, that all biological agents provided in the scenarios are aerosolized, so they are inhaled and

retained in the respiratory tract, because it is the most effective way of biological attack. It is fast, uniform, covers a large area, so a maximum number of potential victims, and what remains in the air will deposit and contaminate the soil and objects in the area, which will become secondary sources of contamination.

The human response is considered to be at full dose exposure to the CBRN agent, but the latency period is variable depending on the individual, especially for the biological agents. It is considered that the reaction of the organism exposed to biological agents can be mathematically modeled according to the probability of the dose/disease or death relationship, with a time distribution of the incubation period and the duration of the symptomatic disease. The mathematical distribution of the duration of the disease differs in survivors and non-survivors, and the period of the individual's illness is divided into stages, depending on the level of severity. These simplifications and generalizations of the infectious process (which in reality is complex and multifactorial) allow the practical estimation of the severity in time of the infectious disease, namely *the dynamics of the effect.* It is believed that the biological agent infects all exposed people, but to varying degrees, from subclinical (asymptomatic) to lethal. The methodology includes the *infectivity submodel* which describes the relationship between the inhaled dose and the probability of disease, respectively the "infectious dose" in living microorganisms and the "effective dose" in toxins, as well as the severity of the disease. (NATO AMed-8(C), 12-13)

Prophylaxis, in this methodology, is considered to be applicable to infectious diseases caused by non-contagious biological agents in whom there is a vaccine, (for example, anthrax) as an optional parameter in the scenario. The inclusion of prophylaxis in the calculation may give underestimated results, as it does not take into account the individual reactivity and the infectious dose. For other biological agents the methodology does not take into account prophylaxis, if there is no effective and/or available vaccine. (NATO AMed-8(C), 12-13)

Use of methodology

The methodology for mathematical estimation of health and total losses in biological attack is used by NATO for training and medical, logistical, operational, personnel management planning. (NATO AMed-8(C), 16)

Medical planning, by estimating cases, identifies the medical requirements for each "medical role" separately: drugs, medical devices, type of beds, staff specialty (AMedP-7, STANAG 2478, and AJP-4.10).

Logistics planning determines the medical and non-medical logistical requirements that are necessary for the management of CBRN pathology, with the supply and resupply of specific materials (AJP-4).

Operational planning estimates the ability to evaluate the performance of actions, including parameters such as: health losses, total human losses, individual and collective physical protection, necessary medical countermeasures and even avoiding the operation. (AJP-3).

Personnel planning estimates the need for replacement personnel for CBRN victims (sick and deceased) (AJP-4.10).

The methodology for estimating the effects of biological attack with non-contagious agents details the human body's response to various pathogens, contagious and non-contagious WBA, which are taken into account in the work scenario.

Peculiarities of the biological attack

The WMD CBRN attack can have catastrophic effects if the military is not properly prepared, trained and equipped. In order to reduce the effects of CBRN agents on the troop, it is necessary for planners/commands to estimate as accurately as possible the total and health

losses that would occur in different scenarios. Biological attack has its own peculiarities, which differentiate it from other WMDs, but there are also differences between the effect of contagious and non-contagious biological agents involving different military scenarios (Tables no. 2 and 3). (Ordeanu Viorel, 2012).

Table no 2: Essential characteristics of the main non-contagious vs. contagious WBAs (took as a representative example)

No.	WBA weapon	Group	Lethal	Contagious	Prophylaxis (vaccine)	Specific treatment	Observations
1	Antrax	bactera	+	-	+	+	
2	VEE	virus	-	-	-	-	
3	Botulism	toxin	+	-	-	-	
4	Pestis	bacterium	+	+	+	+	
5	Smallpox	virus	+	+	+	-	
	index		4	2	3	2	

Tabel no 3: The potential use in biological attacks of main noncontagious vs. contagious WBA (taken as representative sample)

No.	WBA weapon	Group	Tactic	Operative	Strategic	Probability ranking	Observations
1	Antrax	bacterium	+	+	+	**1**	
2	VEE	virus	+	+	-	**5**	
3	Botulism	toxin	+	+	-	**4**	
4	Pestis	bacterium	-	-	+	**2**	
5	Smallpox	virus	-	-	+	**3**	
	index		3	3	3		

Mathematical estimation of human losses caused by biological attack can be achieved by specific methodology, being necessary for medical, logistical, operational and personnel planning. Estimates allow the optimization of medical and non-medical countermeasures to counteract the biological attack and eliminate its consequences.

3. Mathematical modelling of the epidemics induced by biological attacks with noncontagious agents

The methodology for estimating the effects of non-contagious WBA attack is based on the scenario that the disease is caused by inhalation of aerosolized WBA. The human response (the body's response) to the biological agent depends on the dose estimate, as with other CBRN agents, and evolves over time with varying degrees of disease severity, specifically with respect to other agents. The calculation is different for non-contagious and contagious agents, in which the contamination is continued by interhuman transmission (from person to person) and is fragmented into specific submodels, so it is more complex. (NATO AMed-8(C), 13-14)

The infectivity sub-model estimates the number of individuals who will be ill after exposure to the agent dose. The (latent) incubation period estimates when individual signs and symptoms will appear.

The mortality sub-model estimates the number of patients who will die. The duration of the disease is estimated with the set of symptoms until healing or death. The disease profile sub-model describes the different clinical stages of the disease and the severity over time (dynamics).

The body's response to noncontagious diseases is quantified by the number of individuals who will become ill, those who will die, and those who will recover. These values derive from the known parameters of infectivity and mortality known for the respective disease and can be calculated for each military or "n" group (*icon*):
in = number of individuals in the group
dn = dose of agent received by each in the group
pn = efficacy of pre-exposure prophylaxis for the agent, for each group (if not vaccinated the value is 0)
pE(dn) = the probability that an individual in group n will get sick if he receives the dn dose
pf(dn) = the probability that an individual in group n will die if he receives the dn dose.

Thus, the distribution and parameters calculated for the probability of illness and/or death are specific to the agent, and individuals receive the same dose and have the same prophylaxis.

The methodology requires that in all diseases with mortality:

[1] $pf(dn) \leq pE(dn)$ for all n

because the number of deaths cannot exceed the number of subjects, and for non-lethal diseases:

[2] $pf(dn) = 0$

for all values of n and dn, although mortality is not excluded.

The number of individuals in the group which will become ill is:

[3] $En = in \times (1\text{-}pn) \times pE(dn)$

The number of dead people is:

[4] $Fn = in \times (1\text{-}pn) \times pf(dn)$ where:

En = number of ill people in n group,
Fn = number of dead people in n group.

The total number of ill people in all groups:

[5] $E = \sum_{n=1}^{N} En$

Total number of dead people in all the groups:

[6] $F = \sum_{n=1}^{N} Fn$

where N = total number of groups

Total number of survivors is:

[7] $S = E - F$ where:

S = number of survivors
E = number of ill people
F = number of dead people

All these values are calculated daily for those who show signs of disease according to the degree of severity, according to AMedP-8(C).

3.1. Anthrax as a biological weapon

The anthrax bacillus (*Bacillus anthracis*) is a gram-positive bacillus that sporulates, is found in nature in the soil and can cause diseases in humans and animals (zooanthroponosis): cutaneous, digestive, pulmonary, meningeal and/or septic anthrax, with high lethality. In unfavorable environmental conditions it forms spores (resistance form) with a diameter of approx. 1 μm, which can survive for decades. So it can be stored like any other ammunition to be used when needed. The spore itself does not produce sickness, because it has no biological activity, but after entering the body it is hydrated, grows, passes into a vegetative form

(bacterium) that multiplies and secretes toxins, so it provokes complex illness. For operational, technical and medical reasons, bacterium are the favorite biological agent because they are easy to multiply, and among them the spores of *Bacillus anthracis* are preferred. As proof, the attacks at the beginning of this century were committed with *Bacillus anthracis* spores. (JAMA. 1999)

It is considered that aerosolization of *Bacillus anthracis* spores results in an explosive but non-contagious epidemic of anthrax pneumonia. In this way the disease will not spread to the troops, the civilian population or the forces of the attacker, and if it attacks in the place where the front is weakened by illness and death of defenders, there would be no major risk of contamination and infection. Some also consider the aerosolization of pestis bacilli, which causes lung plague, to be a non-contagious disease. From a medical point of view this can only be true from a CBRN point of view. The medical service cannot rely on the assumption that the microbes that cause respiratory diseases are not contagious, it is necessary to apply appropriate countermeasures for the protection of medical staff and other patients. (AmedP-8(C), 2010)

Epidemiologists believe that anthrax has low contagiousness, but patients with lung infection will eliminate microbes through coughing, sneezing, speech, saliva, sputum, bleeding, etc. Around these patients there will be a major risk of air contamination, with a maximum density of up to 1-2 m and a lower risk of up to 7-8 m and contact contamination, direct (interhuman) and indirect (through objects and contaminated surfaces). So patients hospitalized for isolation and treatment will contaminate other patients, health care workers and others, including with lung disease, triggering isolated cases of disease or outbreaks. These patients will not cause a secondary epidemic, but are contagious and endanger primarily the medical staff, who must protect themselves properly and apply measures to prevent airborne contamination and contact. The environment will remain persistently contaminated and require special decontamination/disinfection measures. (Ordeanu Viorel, 2012).

The methodology is based on the scenario that the disease is caused by inhalation of *Bacillus anthracis* spores so it manifests as pulmonary anthrax (inhaler) which in the absence of prophylaxis and treatment has 99% mortality and the incidence of cutaneous and digestive anthrax (which are treatable) is negligible. This results in an underestimation of the total number of patients. According to the methodology (AmedP-8(C)), pulmonary anthrax is considered to be lethal in all cases, therefore

[8] E = F therefore S = 0

The WIA calculation estimates the level of severity of the case, the number of patients per day and the inhaled dose of Ba spores:

[9] D antrax n spores UFC (units forming colonies).

It is considered that the minimum dose of spores for an individual's illness is min. 8,000 viable spores (Dembek, Zygmunt F., 2011).

For the DOW calculation, the mortality of 100% is assumed and the DOW is calculated per day and then the total is made.

Anthrax dose infectivity is modeled as a randomized variable with exponential distribution with the parameter λ (*lambda*):

[10] $PE_{anthrax}(dn) = 1 - e^{-\lambda dn}$ where:

n = number of groups

PE anthrax (dn) = the fraction of personnel exposed to the dose of anthrax that causes the disease

dn = dose of anthrax spores in the group

λ = parameter of response-dose = 1.69×10^{-5} (AmedP-8(C), A-35 – A-36)

It is considered, based on the known case study, that after inhalation of anthrax spores the disease appears after 1-2 days after high dose (over 1,000,000 spores), at 4-7 days at low

dose (10,000 spores), and the danger of illness remains for over 50 days. The disease passes into stage 2 between 3-7 days at high dose and in 9-10 days at low dose, and deaths begin to occur from the second day, with a maximum of 4-7 days at high dose and occur only rarely at low dose, but the risk persists for more than 50 days. The explanation is that some spores can pass late in the vegetative form that causes the disease. As a result, current treatment recommendations EMEA provide antibiotic therapy for 60 days twice a day, both therapeutically and prophylactically after exposure. There are vaccines for human and veterinary use for prophylaxis and if available they protect against disease or reduce the severity of the disease. Post-exposure prophylaxis and treatment are done with antibiotics (preferably fluoroquinolones), but the sensitivity of the bacterium should be checked. Patients should be monitored for at least 60 days, not only for the present infectious disease, but also for relapses as well as for possible side effects of therapy: allergy to antibiotics, side effects of ciprofloxacin, etc. (EMA/CHMP, 2015)

3.2. Viral encephalitis with VEE as a biological weapon

The Venezuelan Equine Encephalitis virus can also infect humans as a non-lethal zooanthroponotic virus, even if it is aerosolized (non-lethal, disabling agent), so theoretically:

[11] $E = S$ and $F = 0$

For WIA, the number of patients is multiplied by the values in tables A45 and A46 in AMedP-8(C). For DOW, the value is 0, because VEE exposure does not cause mortality, so it is no longer calculated. Estimated human response to VEE encephalitis input data:

[12] Inhaled dose VEE = DVEE, n UFP (units forming plates).

Infectivity is modeled with a 100% probability of producing the disease if the dose of 1 UFP is exceeded and mortality is 0%.

Calculation model:

[13] PE VEE (dn) = 1 for dn ≥ 1 UFP where:

n = number of groups

PE VEE (dn) = fraction of persons exposed to VEE dose to the place of the group who will get ill (exposed and infected)

dn = VEE dose to the place of the group (UFP),

and lethality is assumed as zero (F = 0). (AmedP-8(C), A-50 – A-51)

Diseases occur in the first 4 days, less frequently until day 9 and exceptionally after day 21. The epidemic caused by aerosolization of VEE would be similar to influenza and coronaviruses (example Covid-19), for which we have practical medical experience, as opposed to VEE which is an exotic zooanthroponosis, so almost unknown in Europe. There is no vaccine available and no specific recommended treatment.

3.3. Botulinium toxin used as biological weapon

Botulinum toxin is the most toxic substance known and is considered the standard for WBA toxins. In fact, it is a group of 7 protein substances, with variable toxicity, which are biosynthesized by the anaerobic bacterium *Clostridium botulinum*. Under adverse environmental conditions, this bacterium sporulates and can survive in semi-canned and even canned foods. Once in the body, the spore passes into a vegetative form, multiplies and secretes toxins, which give botulinum intoxication (botulism).

The toxin can be extracted from bacterial cultures, is purified and conditioned as a toxic substance for the production of reagents, drugs and WBA. The presentation of the calculation for botulinum toxin is also a model for the other WBA toxins, which behave similarly to each other and act somewhat similarly to toxic battle substances (WCA). If the toxins are aerosolized,

after inhalation they reach the airways and enter the bloodstream directly from the lungs, so the effect is faster and stronger than if they were ingested. (JAMA, 2001)

Botulism is a lethal intoxication, with a severity proportional to the absorbed dose, with deaths and survivors, for which the rate of illness per day must be estimated, so:

[14] $S = E - F$

In botulism, the WIA calculation is given by the dose-dependent severity level for survivors and deaths. The first stage is of low and medium severity and the number of patients is calculated by multiplying the values. The second stage is severe, and it is calculated by multiplying the number of patients by the values in table A42 for survivors and A43 for non-survivors. For DOW, the values, non-survivors are calculated.

Estimation of the human response to botulism, for input data:

[15] D botulism n µg/om

Botulism diseases are modeled according to log-probit (logarithmic probability) and the median effective dose ED50 = 0.1 µg/person, with a logarithmic distribution that cumulates the distribution of CDF functions:

[16] $PE\ botulism\ (dn) = \frac{1}{2} + \frac{1}{2}\{erf(\frac{\ln(dn) - \mu}{\sigma\sqrt{2}})\}$ where:

n = number of groups
PE botulism (dn) = fraction of people exposed to the dose and getting ill
(dn) = toxin dose µg/om
µ = log natural variable (ln 0.1 µg/human = -2.3026
m = probit (logarithmic probability) 1/m 1/12.9
σ = standard deviation of natural logarithm e where = e = 1.0806
erf = function error, namely:

$$erf(x) = 2/\sqrt{\pi} \int_0^x e^{-t^2} dt$$

Lethality in botulism is given by formulla:

[17] $PF\ botulism\ (dn) = \frac{1}{2} + \frac{1}{2}\{erf(\frac{\ln(dn) - \mu}{\sigma\sqrt{2}})\}$ where:

PF = fraction of people exposed to the dose and dying (percentage mortality). (AmedP-8(C), A-43 – A-49)

The disease appears from the first day (short latency), after 4 days the number of new patients decreases until day 19, but isolated cases can also appear after 21 days. The lethality is high in the first 2-5 days, then decreases to 21 days, after which sporadic deaths can be recorded, for which there is still no physiopathological explanation. There is no vaccine available and no specific recommended treatment.

Conclusions

In the case of a WMD CBRN attack that also uses biological agents, it is most likely to be used non-contagious WBAs to infect, lethal or non-lethal, as many military personnel as possible, but without creating the risk of contamination for the attacker's troops as well.

Mathematical modeling of the epidemic induced by biological attack (number of sick and dead people) with non-contagious agents is useful for planning the forces and means of medical service, for planning offensive or defensive operation, logistics and human resources needed for support and replacement. The estimates resulting from the calculations according to the formulas recommended in the specific documents allow the optimization of the medical and non-medical countermeasures for the liquidation of the consequences of the biological attack.

BIBLIOGRAPHY:

***, AJP-4 Allied Joint Logistic Doctrine.
***, AJP-4.10 Allied Joint Medical Support Doctrine.
***, AJP-4.10 Allied Joint Medical Support Doctrine.
***, AJP-43 Allied Joint Operation.
***, Concept of operations of medical support in Chemical, Biological, Radiological, and Nuclear environments.
***, EMA/CHMP. 2015. Guidance document on use of medicinal products for the treatment and prophylaxis of biological agents that might be used as weapons of bioterrorism, European Medicines Agency.
***, NATO AMed-8(C), Introduction, 1-18
***, NATO AMedP-8(C), Basis for injury profiles, C-1-95, 2.
***, NATO Planning guide for estimation of CBRN casualties – AmedP-8(C), A-34 – A-42, A-35 – A-36.
***, NATO Planning guide for estimation of CBRN casualties – AmedP-8(C), A-50 – A-51
***, NATO Planning guide for estimation of CBRN casualties – AmedP-8(C), A-43 – A-49
***, North Atlantic Treaty Organization (NATO) Planning Guide for the Estimation of CBRN Casualties- AMedP-8(C). 2010
***, STANAG 2478, Medical support planning for Nuclear, Biological, and Chemical environments.
DEMBEK, Zygmunt F. 2011. USAMRIID's Medical Management of Biological Casualties Handbook, 7th edition. Fort Detrick, Maryland, USA: Army Medical Research Institute for Infectious Diseases (USAMRIID).
JAMA. 2001. "Botulinum toxin as a biological weapon". Consensus statement. Vol. 285, No. 8, February 28, 2001.
ORDEANU V. (coordinator). 2012. Protecţia medicală contra armelor biologice şi a bioterorismului. Bucureşti: MApN CCSMM (In English: Medical protection against biological weapons and bioterrorism).
ORDEANU, V., ANDRIES, A.A., HINCU, L. 2008. Microbiologie și protectie medicala contra armelor biologice" Bucuresti: Ed. Universitara "Carol Davila" (In English: Microbiology and medical protection against biological weapons).
ORDEANU, V., NECSULESCU. M., IONESCU, L.E., POPESCU, D.M., BICHERU, S.N., Dumitrescu, G.V., Hertzog, R.G. 2008. „Anti-infective Therapy Principles in Diseases Caused by Bacterium Biological Agents". Journal of Pharmaceutical Research International, 23, 5.
ORDEANU, Viorel (coordinator). 2012. Protectia medicala contra armelor biologice (manual pentru pregatire postuniversitara), Bucuresti: Centrul de Cercetari Stiintifice Medico-Militare (in English: Medical protection against biological weapons (manual for postuniversity education).
ORDEANU, Viorel (coordinator). 2012. Protectia medicala contra armelor biologice - vademecum, Bucuresti: Centrul de Cercetari Științifice Medico-Militare (In English: Medical protection against biological weapons – vademecum).
ORDEANU, Viorel, Profesorul Cantacuzino – o carieră de excepţie, Viața Medicală, April 2021.The European Agency for the Evaluation of Medicinal Products. 2002 (updated 2007). CPMP/4048/01. EMEA/CPMP Guidance document on use of medicinal products for treatment and prophylaxis of biological agents that might be used as weapons of bioterrorism, London.

DOI: 10.53477/2668-6511-22-05

COMBATING PANDEMICS AND SOCIAL INTERACTION ERRORS – MOVIES VERSUS REALITY

Ioana-Flavia DRĂGOIANU,
Bachelor's degree student in Security Studies, Faculty of Political Science,
University of Bucharest
E-mail: flaviadragoianu@yahoo.com

Abstract: *One of the major security threats Humankind was confronted with, along several millennia, was coping with deadly viruses. In such a situation, different means of protection of the population have been ensured – medical discoveries, vaccines, and social interaction obstructions. As the creativity of man knows no bounds, different scenarios have emerged regarding combating disease whilst many scientists have designed layouts of coping with deadly viruses, using different models of infections. The goal of this paper is to analyze some of these models, through the lens of Security Studies and Political Science. Then, the discussion will shift towards social interactions and manipulating the social network. Furthermore, we will apply this model on a few selected movies, critically comparing them to the reality we are facing today. Thereby, the focus shall shift towards four well known movies: Contagion (2011), Outbreak (1995), Quarantine (2008), It comes at Night (2017) and their approach to containing and curing viruses, while also quenching the impeding chaos of dismay.*

Keywords: *pandemics; chaos; social interaction; social network; exclusion.*

Introduction

To understand how a pandemic and an infectious disease work, I deem important an understanding of these terms. The first use of the word pandemic belongs to a Dutch physician, Gideon Harvey, who in 1674 wrote "Morbus anglicus or a theoretic and practical discourse of consumptions and hypochondriac melancholy" and later, the erm was used in 1828 by Noah Webster in the "American Spelling Book". (Cavaillon, 2021, 1-2)

During ancient times, people were not able to determine the causes of disease. Thus, disease became both a cause of divine punishment in the eyes of some and an unknown force of calamity in the eyes of others. The Great Pestilence (Cocoliztli epidemic) is considered one of the deadliest outbreaks of all times, but its cause remains a mystery over five hundred years later, as no known pathogens match the symptoms. The inevitability of disease has been a far-reaching subject: from depictions of skeleton-like figures claiming the lives of beings to stories of pandemics and their unescapable grasp. (For instance, *The Masque of the Red Death* by Edgar Allan Poe). It is certain that it has become an important aim of mankind – to discover, analyze and eradicate such a substantial threat to human security. Not understanding the cause and the "mechanism" behind sickness, humans developed strategies of defending themselves against unseen dangers. Masks, isolation, quarantine and eventually vaccines became the foundation of preventing or stopping outbreaks right in their tracks.

Finally, as long as development is possible, new threats to the welfare of humanity come to light – one such threat is the continuous advancement of diseases. Its emergence has been a constant in history and for as long as we know, it has always seemed like an invisible and unstoppable threat. One of the main agents of infection is the spread through pathogens belonging to animals, that further sustain human-to-human transmission.

1. The world we know and the social network

Further, we will be discussing some hypothesis that will become our basis in judging the accuracy with which measures of combating a pandemic is portrayed in movies.

Social interaction is unmistakably one of the necessities a human requires – but it is always the fastest way through which a virus can spread. I consider it relevant to evoke the model of Daniel Bernoulli, due to the fact that he can be considered the first to use a different equation in order to deduce formulae, leading him to the idea of statistical hypotheses in order to create models for various premises. (Sheynin, 1977, 105) He divided the population into two categories: susceptible (the ones yet to be infected) and immunes (the ones who are immune all their lives). Only a part of the entire population survives to become immune, and the percentage varies in accordance to the disease. The probability of surviving is inversely proportional with the death rate and the force of the pathogen, but there are other factors that come into equation such as age, other infections already present and susceptibility. Although the mathematic models of Bernoulli are focused on smallpox, they represented an important tool in understanding infectious disease epidemiology.

A more recent study is the one Laura Glass started as a fourteen years old girl. She used an agent-based model to describe how a disease spreads using a detail of vital importance – social interaction. Influenza became her and her fathers, Robert Glass' focus, as a relatively common infectious disease and a pliable subject of research. I find their study more relevant due to the possibilities they subject in their work, analyzing not through mathematical notions but through the eyes of a modern and observing onlooker.

Social networking opens a whole world of possibilities, as it is formed by groups of people who can easily infect each other, especially given the fact that one person may belong to more than one group. Taking the case of Influenza, an infected person can become infectious in presymptomatic state or in an infectious asymptomatic state. (Glass, 2006, 1672) and having contact with the outside world keeps the circle of infections complete, as asymptomatic carriers can possibly infect others without realizing. However, a symptomatic person more often than not becomes immune, but in some cases, may even die.

The pair deems teenagers and children as the most important chess piece. During their studies *for influenza as infectious as 1957-58 Asian flu (≈50% infected), closing schools and keeping children and teenagers at home reduced the attack rate by >90%.* (Glass, 2006, 1671) This statement opens a new hypothesis to be put to analysis – how the social network changes and how we can manipulate it in case of a pandemic. One way through which we can slow down a pandemic is by exclusion – as long as an infected person does not have contact with others in the network, they cannot infect further. This happens through the severing of the individual from the network. Consequently, social distancing becomes an important practice but also a challenge. Its purpose is to control the spread of the disease until a better solution, like inoculation, is present. But what happens when not even seclusion can be upheld?

This leads us to another important premise – how much of a Superspreader is behavioral misconduct and how much is a genetic outcome. As mentioned earlier, from the dawn of time humanity has tried combating disease through different methods. A representative case took place in the fourteenth century, when people tried to control the spread of the Black Death through quarantining, socially distancing and wearing masks (for instance, the beaked masks filled with strong-smelling flowers, such as lavender). However, during present day COVID-19 pandemic, we often notice these older, but still effective, rules are not being respected by all in social networks all around the globe. It is enough for a handful of people from a network to not wear masks for the disease to gradually reach more and more people. This leads to a major problem, because *if the daily incidence surpasses the treatment capacity, it will overwhelm the*

healthcare system with detrimental consequences for medical care of infected individuals and increased mortality and morbidity. (Catching, 2021, 4) This situation could be seen in Italy[1] and Romania[2] during the COVID-19 pandemic. During an analysis of masks' efficacy, it has been discovered that it could range "anywhere from 20 to 80% for cloth masks, with ≥50% possibly more typical (and higher values are possible for well-made, tightly fitting masks made of optimal materials), 70–90% typical for surgical masks, and >95% typical for properly worn N95 masks" (Eikenberry et al, 2020, 298).

Further, we shall discuss the validity of four movies regarding real-life practices, behaviors and decisions, whilst implementing the ideas exemplified above.

2. How imagination may become reality

The first three movies we will center our attention on are *Contagion* (2011) *Outbreak* (1995) for their focus is how the world shifts to combat a high infectivity and mortality rate disease. The way the infection bursts and spreads, the steps the decision-makers take, population's reactions, the implication of military control and ultimately, solving the issue will be studied. We will also discuss *Quarantine* (2008), which focuses on a smaller scale of events. However, the last movie, *It Comes at Night* (2017), will give a glimpse to a different kind of situation, where the spreading of the virus could not be contained. Therefore, the focus will not be on the protocol following an outbreak, but on the mechanism and psychology of a social network during one.

Contagion (2011) tells the story of a bat-borne virus, MEV-1, that destroys the peace and quiet of the world. The first person we are introduced to, Beth Emhoff, is in the middle of interacting with different kinds of groups. She is one red dot in the green of the social network, as she is the index case (Patient 0). This brings an insight to the importance of interaction in the network, and to one of its immediate characteristics – it is unavoidable. The struggle to restrict social interaction brings forth the issue of families, where spreading a disease is extremely easy. We see that happening in the movie in the Emhoff family, as the mother and son die, while the father discovers he is immune.

Meanwhile, the Centers of Disease Control and Prevention (CDC) begin tracing the path of the virus – every person coming in contact with the first case discovered becomes a priority. Mapping the disease through the interactions a person becomes a priority and one of the first steps to be taken in understanding how the issue of the virus is evolving. We can see the same approach, but at a smaller scale during the Thomashefsky Case, where the social history of the woman who first came in with a case of Hepatitis C is meticulously reconstructed – from every place she visited to the people she came in contact with.

One of the most important scenes is the one where the father, Mitch and the daughter go into a store, where they encounter an infected woman that uses no means to protecting herself or the others. She coughs over the products and towards people around her, becoming a Superspreader. The behavior she exhibits is accurate, for we can also notice the same kind of carelessness in some cases during the COVID-19 pandemic.

[1] A.N: Italy faced excess mortality and morbidity during the pandemic – this is illustrated by the analysis of 2020, when the excess mortality reached 15,6 %. (Dorrucci, Minelli et al, 2021, 3) and by the rise in weekly infectivity cases from the 9th of November, reaching 19, 002. (WHO, 2021)

[2] A.N: In Romania, the excess mortality reached 62,6% in November 2020. Nota bene: Excess mortality is expressed as the percentage rate of additional deaths in a month, compared to a "baseline" in a period not yet affected by the pandemic. The baseline adopted consists of the average number of deaths that occurred in each of the 12 months during the period 2016-2019. (Eurostat, 2021). Regarding confirmed COVID-19 cases, by 11th of November 2021 there can be identified 90,183 cases per million people. (Our World in Data, 2021).

Chaos is an element I find extremely important in the situation of an outbreak, as it brings with itself uncertainty. The protocol seems simple to follow – stay inside, stay calm, limit social contact, be careful not to infect and not to be infected while a cure is in developing. But some people are disobeying of the rules and have proven to be quite selfish in these situations. Hence, the first instinct is self-preservation, causing people to do anything to survive, even if it is in detriment of another. We see the effects of panic and desperation clearly, mirrored into reality.

During the start of the COVID-19 pandemic, in 2020, the world found itself in a similar situation when stores were assaulted by the population, looking to stock up as many items as possible. The same chaos can be seen at a larger scale during the movie, while entire cities enter lockdowns and people try to leave in order to escape both the disease and restrictions that follow.

Quarantine (2008) is focused on a news reporter, Angela Vidal and her cameraman who are documenting the work of the Los Angeles Fire Department. An emergency call brings them to an apartment building where screams and loud sounds were reported, and unbeknownst to them, a place riddled with a virus similar to a mutated form of rabies.

The first action towards containing the virus to be witnessed is locking down the building. No one can get in or out. The purpose of this action is to stop a future disaster by separating the infected ones from the social network, making it impossible for them to infect others. Separating individuals entirely from the network has proven itself effective, especially during the lack of a vaccine, and the military plays a major role towards maintaining the severance.

Being stuck inside, the firefighters ask the tenants to group. Scrutinizing this decision, we can deduce that by gathering all the people in the same room we are putting the uninfected in danger. They do not know what they are facing and the decision to bring together the people of the apartment building can cause the infection of all. Keeping the tenants separated in their apartments would have been the best solution for a positive outcome, as even the rabid would not escape the confinements. The corroboration of the statements is offered later during the movie, when a mother and daughter show symptoms.

After dealing with threats when they try to leave, the CDC sends two officers in hazmat suits to analyze the situation from inside. They decide to cuff the injured people as a safety measure, which is a benefiting decision since the virus makes them aggressive. However, it does not assure their safety, as one of the CDC officers is bitten and infected. Shortly after this scene the mapping of the virus is revealed, as well as the index patient – a dog, that was taken to the veterinary and infected other dogs, who in exchange turned aggressive and bit their owners, transmitting the mutated rabies. Afterwards, the original infected dog is traced back to the apartment building by the CDC, resulting in the lockdown. We can consider that the mapping of the virus is accurate, but it was relatively slow.

Furthermore, facing an unknown virus and seeing themselves under lockdown, chaos ensures. We see the people trapped in the building not thinking clearly. The remaining people of the group tie the infected mother of the girl to the staircase, thus blocking the narrow hallway, restricting the space even more. They have successfully trapped themselves between a room with rabid humans, an exiguous hallway and a staircase that leads to more infected tenants. The decision to sedate the little girl, now fully into a rabid state, proves itself faulty, as that means they had to go to the next floor, pass the woman cuffed to the stairways, and enter a space filled with rabid tenants. This choice serves as a turning point due to the fact that they are caught between the newly infected couple of people they sent to the next floor and the rabid CDC officer that managed to escape through a poorly barricaded door.

The chaos caused by the group's deficient decisions and the lies the rest weave to save themselves, knowing they are infected, leads to the final of the movie. In the end, no one manages to escape the building, succumbing to the mutated disease that is discovered to be named the Armageddon Virus. In this case, becoming immune was an impossible task, as rabies cannot be cured after symptoms start surfacing, and the virus takes only a few hours to fully take over.

Outbreak (1995) has a different approach to the other two, being focused even more on the decision-making necessary in such situations and the involvement of the military. As soon as the Motaba virus emerges in South Sudan, two U.S. Army Officers make the decision to keep it a secret and contain it by destroying the small camp of infected soldiers. Considering the 100% mortality rate and lack of vaccine, the morally difficult decision drops the possibility of a devastating outcome. In this case, the immunity of the remaining population was acquired through the death of the infected.

However, the Motaba Virus resurfaces through a capuchin monkey, which causes a chain reaction. The situation takes a turn for the worse when it mutates into a virus that spreads in a similar manner as Influenza. The inspiration for the disease is the Ebola virus, which emerged in 1976 in Africa and became a global epidemic within months during 2014- 2016.

A significant scene is the one when the United States Army Medical Research Institute and its levels are presented. On the last level, containing high mortality viruses, we see one of the workers take off her mask before leaving the area. Since the virus can be all over the gear, it must be carefully disposed of, and taking off a mask in the laboratory is not a wise choice. It gives us an insight on how much of a small mistake can impact a greater level.

Another important scene is the one where an infected man enters a cinema serving area and asks for water, whilst not wearing a facemask. The superspreaders are very common during the movie, most of the sickness being transmitted due to wrong behavioral reasons. This leads to a situation mentioned previously – the inevitable overwhelming of the healthcare systems. The virus continues to spread through the hospitals due to the deluge of patients. Civil unrest is also depicted, chaos starting engulfing the population desperate for a cure.

The CDC's portrayal is of great importance. They try to locate the origin of the virus in order to create a social history of the deadly disease. The mission seems impossible, as there have been numerous transports of capuchin monkeys. Not only do they have to find the right one, but to also identify the first monkey to have been infected. The models of the Motaba Virus they create are very accurate and show how the healthy cells are slowly taken over, making it impossible for them to reproduce.

The movie brings a different approach through the origins of the Motaba Virus, which is revealed to have been constructed as a bio-weapon. In the end, a vaccine is released and the pandemic is quelled. The 100% mortality rate can also be considered a hinderance in the process of spreading, as it is possible for the person to die before they get to infect others, but the high infectivity level can also lead to a situation when people are being rapidly infected, even in a short amount of time.

On the other hand, the movie *It Comes at Night* (2017) shifts our focus from what happens in the bigger picture to the smaller pieces of the puzzle. After an unnamed disease leaves Earth in ruins, a couple and their son's survival is related. An important detail is the place where they decide to live, a cabin deep in the woods – a self-sufficient and most importantly, secluded, decision. By limiting the need to interact with others either through avoiding needing stores and communicating to individuals, the family has successfully cut itself from the network and lowered the chances of being infected. Secluded and stocked up houses are a big part of the survivalist movement, where preparing for emergencies either through long-term or short-term decisions is meant to give an advantage in case of catastrophe.

One of the important scenes we see early in the movie is the when the grandfather gets sick, as he is immediately killed and his body is burned in order to prevent the transmission of the virus.

A relevant scene, and the catalyst of their downfall is accepting another family in their home. Such a dangerous decision comes with consequences, as they do not know if the people they are about to welcome in their own home are infected or not. Admittedly, in an almost apocalyptic world, defense against other groups is easier when there are more people, but so is spreading the virus. Knowing that of the others find out you are infected would bring an even more premature death, and death is one of humanity's greatest fears, one individual's judgement can be clouded, putting at risk the entire group.

There are two families now living under the same roof: the couple Paul and Sarah and their son, Travis, and the newcomers which consist of the couple Will and Kim, together with their son, Andrew.

The turning point of the movie is when Travis leaves the safety of the house and brings back their missing dog, leaving the door unlocked. Paranoia and fear start changing the dynamic of the social network that was created between the two families. They start doubting and suspecting each other, leading to them quarantining in separate rooms. This scene represents one of the last rational decisions before fear of infection. The human behavior under the looming threat of being infected and killed is perfectly portrayed, reaching its zenith when Andrew is suspected and they decide to kill the newcomers. By eliminating him from the network, just like in the case of the grandfather, they boost their chances at survival. At the same time, it is never revealed if they were indeed infected or the desperation and self-preservation took over the household. Travis soon follows, dying because of the virus. The movie ends with a scene showing the sickly-looking parents standing at the table.

3. Responding to a crisis

One key factor that binds the four movies consists is the existence of errors: in social interactions, mappings, practices and so on. Errors have become a part of human life. Errors in judgment can be seen as the turning points in every movie previously analyzed: the choice to group with people when there is a possibility for them to be infected, removing masks at the wrong time or even not wearing any. But we also see another side that is reflected in our world – malpractice. As shown in *Contagion* (2011), Patient 0 is infected as a result of the cook not washing his hands. A similar situation can be seen regarding the Thomashefsky Case (2015), that we have previously only analyzed as a mapping example. The lack of gloves, unprepared staff, undated blood vials and chaotic placement of dirty vials besides clean ones was enough evidence to shut down the clinic. Officials notified the patients who received injections from the doctor from 2008 to 2015. (Staff, 2015)

Social networking is accurately represented, especially comparing movies with reality. We may take COVID-19 as an example - after the outbreak, authorities of the first affected countries imposed quarantining along with certain restrictions, but under different intensity and results. The Oxford Covid-19 Government Response Tracker was successful in representing in a chart the Stringency Index of various countries, as it can be seen in Figure no. 1:

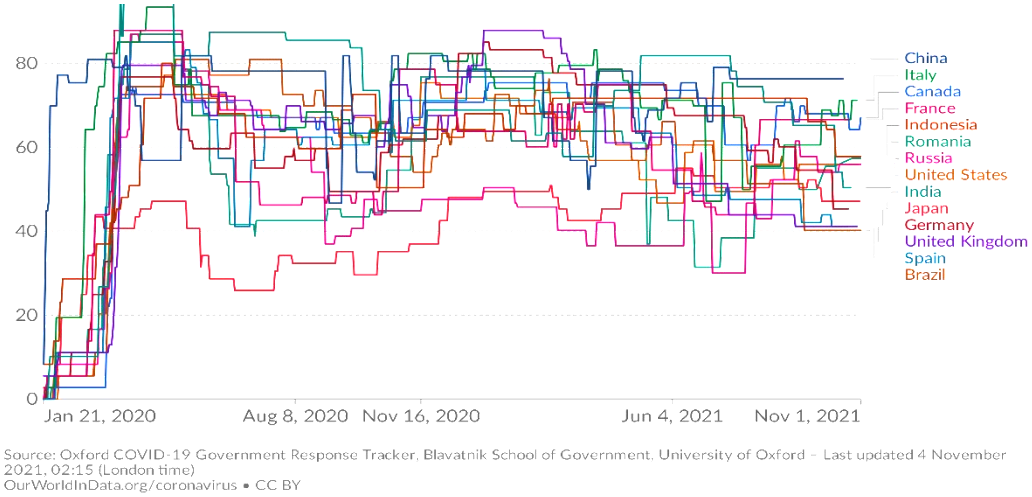

Figure no.1: COVID-19 Sringency Index (*OxcCGRT)*

We can see that China and India maintaied the strictest policies against Covid-19 for a very long time, until aproximately the 20th of September, 2020. Italy, the United Kingdom and Germany take their place until the 11th of May, 2021. Despite the complicated and changing positions on the chart, we notice that China, India and Italy are the most constant out of the 10 countries tracked. The scale rates the severity of the restricitons imposed.

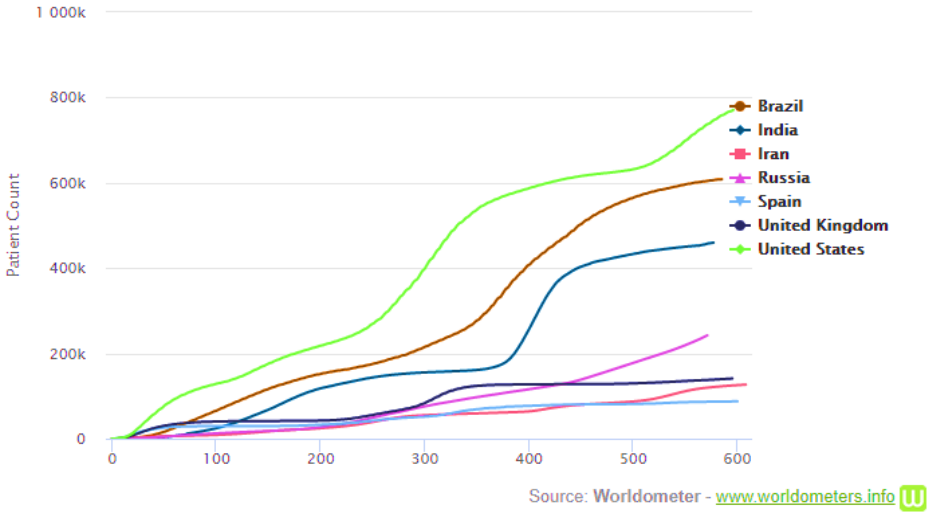

Figure no. 2: Cumulative number of deaths, by number of days since 100 deaths (Worldometers)

For a better understanding we may compare the Stringency Index with the mortality graph in Figure no. 2. It can be easily observed that the United States, which imposed lighter restrictions, also had a higher infectivity rate, especially compared to the United Kingdom's harsh approach at that point that led to low mortality and infectivity rates. Following the REUTERS COVID-19 global tracker we can also notice that Asia and the Middle East have a lower infectivity and mortality rate (at its peak, around 700k infections and respectively 12k deaths) compared to Europe, who peaked at little over 800k infections and 17k deaths.

We can deduce that separating individuals to decrease the rate of infections is effective, but only as long as the indications and separations are followed. As previously mentioned, there are people that are by behavior what we know as superspreaders. As we have seen during the COVID-19 pandemic so far, superspreaders are commonly the individuals who do not follow the restrictions imposed. Hence, the probability they become infected and pass it on others is notably higher.

Medical Martial Law in not to be ignored, although it may be considered a tricky concept to define in the case of pandemics, as it refers to the direct involvement of the military in keeping order and making sure every curtailment is followed. We have seen it happen in the movies *Contagion*, *Quarantine* and *Outbreak* as a last resort to keeping the population calm in the face of something they had never experienced before. Although we have seen the Martial Law enacted in order to quell riots and sometimes even social unrest after attacks[3], a medical Martial Law has yet to be enacted. Essentially, when the government fails, the military is tasked with assuming responsibility, even if that means taking initiative in stopping the spread of a disease. That does not mean, however, that the military cannot partake in overseeing vaccination campaigns. In Canada, Brigadier General Krista Brodie is tasked with overseeing the delivery and distribution of vaccines.

Vaccine campaigns constitute an important matter to put under a magnifying lens. In the movies mentioned above (excluding *It Comes at Night* and *Quarantine*) we can clearly see an ideal scenario – everyone is willing to go through inoculation. One may argue that the circumstances differ, as the lethality rate of the diseases mentioned is 100%, but it is also impossible to ignore the death count our present pandemic has. This reluctant behavior has been attributed to a large number of factors, such as misinformation and disinformation, mistrust both in the government and the vaccine itself, rumors, insufficient medical data available at the time and so on. World Health Organization (WHO) created a chart of recommended interventions in order to aid states in managing the pandemic that can be seen in Figure no. 3.

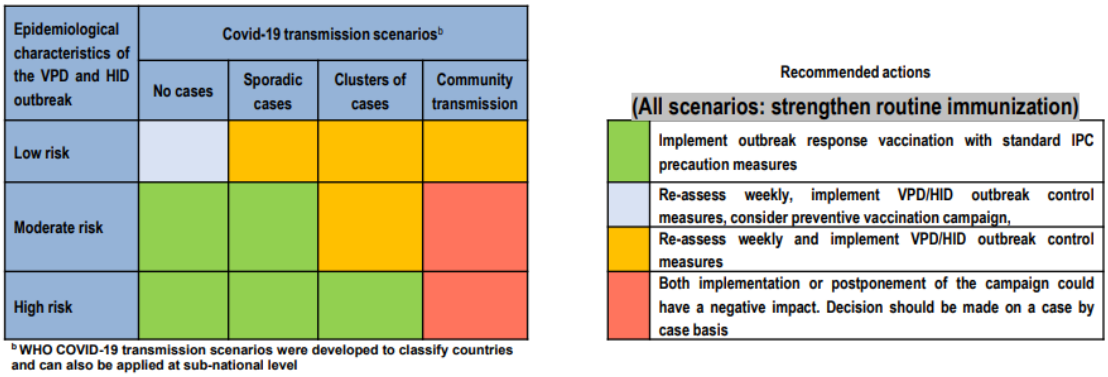

Figure no. 3: Recommended actions regarding COVID-19 transmission scenarios, (WHO)
*VPD – Vaccine Preventable Disease; **HID – Highly Infectious Disease

Despite the attempts at community engagement and displaying information, we can notice that the recommended course of action was not always followed, and combining this with a general misinformation we can see the contributing factors leading to wariness. We can

[3] A.N: There are numerous examples of martial laws being declared, such as: The San Francisco martial law from 1906 after an earthquake and the martial law that followed the attack on Pearl Harbor in 1941. By studying these examples, it can be easily seen how the martial law can be applied on different situations, be it a natural disaster or war.

take as an example the rumors circulated by Taliban that Western vaccines cannot be trusted, leading to a low vaccination rate at the Pakistan borders. (PLOS, 2011). We can add to the growing list of concerns some failed drug trials, such as Trovan by Pfizer, which was supposed to cure the meningitis outbreak in 1996 Africa. (Smith, 2011; Lenzer, 2006, 1233; BBC, 2011)

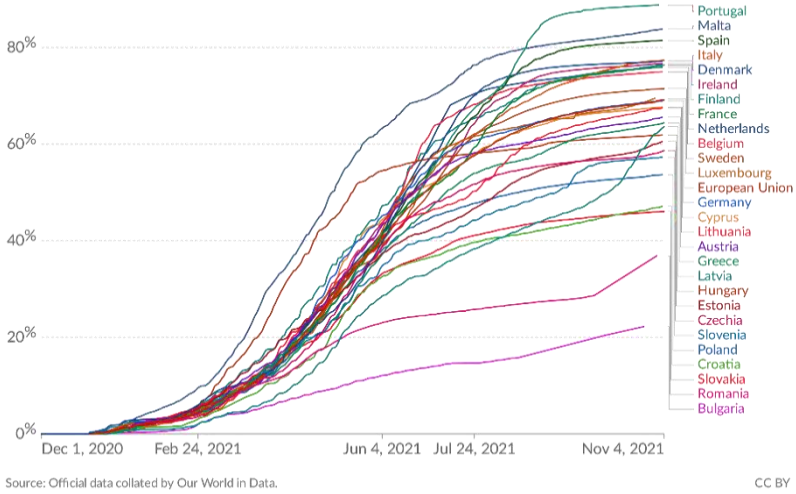

Figure no. 4: People who received at least one dose of COVID-19 vaccine
(Our World in Data)

As we can see, there is a contrasting difference between what is portrayed in movies and reality.

Lastly, along with issues regarding the management of the COVID-19 pandemic there comes another major concern – the psychological state of the citizens. As mentioned previously, in such situations it is not uncommon for an individual to lose rational thinking, maybe even becoming paranoid. Unfortunately, fear induced by extensive mass media coverage of the pandemic may contribute to this as well. There is also the issue of depression due to lack of social interaction, fear of contagion, uncertainty regarding the future, economic difficulties. Moreover, we can notice an increase in anxiety and divorce rates[4] around the world. It is an interesting matter to analyze.

On the positive side, taking Germany as an example, studies concluded that suicide rates were at their lowest during severe restrictions – this has been attributed to the strengthening of familial bonds during lockdowns. (Radeloff, Papsdorf et al, 2021, 3) It is also worth mentioning that this has also been attributed to the increase in social cohesion during threats (Durkheim, 2005; Claassen et al, 2010). Howbeit, this may not be the case in every country.

Conclusions

Out of all the movies, Contagion shows the best representation of an actual pandemic, easily being compared to historical experiences. The mapping and analysis of the virus is accurately portrayed, and so are the decisions taken and the reactions of the citizens.

As we have seen, there were similarities and differences between how humanity imagined combating a pandemic and the actuality of present-day struggles. The psychological and social impacts of such a situation are outlined in both reality and movie-making, but that

[4] A. N.: For instance, the divorce rates in both China and USA grew exponentially during the pandemic. (Prasso, 2020; BBC, 2020)

brings us to certain worries that linger: oftentimes, technology is not able to fully aid us in our quest of eradicating disease. And this is a starting point for even more premises.

We have noticed the tendency towards developing weapons of mass destruction, and biowarfare may be an important element in the future. Whilst a nuclear bomb can be easily traced, a virus is a lot easier to be used in more than one place at once, while guaranteeing anonymity behind a wall of assumptions. This idea is not only explored by *Outbreak* movie, but also in books such as *Future War and Defence of Europe* by John Aleen, Fredrick Hodges and Julian Lindley-French, where COVID-19 is reused years later as a biological weapon.

Times are changing, and in the future we may look at a different approach towards pandemic management, curing disease and the culture of infection prevention.

BIBLIOGRAPHY:

***, BBC NEWS, 2011, Pfizer: Nigeria drug trial victims get compensation, URL: https://www.bbc.com/news/world-africa-14493277

***, BBC, 2020, Why the pandemic is causing spikes in break-ups and divorces, URL: https://www.bbc.com/worklife/article/20201203-why-the-pandemic-is-causing-spikes-in-break-ups-and-divorces

***, Eurostat, 2021. Excess mortality – statistics. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Excess_mortality_-_statistics&oldid=509982# Excess_mortality_in_the_European_Union_between_January_2020_and_August_2021

***, Our World in Data. 2021. Cumulative confirmed COVID-19 cases per million people, URL: https://ourworldindata.org/coronavirus/country/romania

***, Our World in Data, People who received at least one dose of COVID-19 vaccine, URL: https://ourworldindata.org/explorers/coronavirus-data-explorer?yScale=log&zoom ToSelection=true&facet=none&pickerSort=desc&pickerMetric=total_vaccinations&hideControls=true&Metric=People+vaccinated&Interval=Cumulative&Relative+to+Population=true&Align+outbreaks=false&country=European+Union~ESP~FRA~DEU~POL~NLD~HUN~ROU~BEL~PRT~GRC~CZE~AUT~SWE~DNK~IRL~HRV~BGR~SVN~LVA~EST~CYP~MLT~LUX~SVK~LTU~ITA~FIN

***, World Health Organization, 2021, Italy, URL: https://covid19.who.int/region/euro/country/it

***, World Health Organization, Framework for decision-making: Implementation of mass vaccination campaigns in the context of COVD-19, URL: https://www.who.int/docs/default-source/coronaviruse/framework-for-decision-making-implementation-of-mass-vaccination-campaigns-in-the-context-of-covid19-slide-deck.pdf?sfvrsn=438dccc8_2

ALEEN, John, HODGES, Fredrick, 2021, Lindley-French, Julian, Future War and Defence of Europe, USA: Cambridge University Press.

CATCHING, A., CAPPONI, S., Yeh, M.T., 2021, Examining the interplay between face mask usage, asymptomatic transmission, and social distancing on the spread of COVID-19. Sci Rep 11, 15998.

CAVAILLON, Jean-Marc, OSUCHOWSKI, Marcin, COVID-19 and earlier pandemics, sepsis, and vaccines: A historical perspective, Elsevier B.V., Journal of Intensive Medicine, 2021.

CLAASSEN, CA, CARMODY, T, STEWART, SM, BOSSARTE, R.M, LARKIN, GL, WOODWARD, WA, TRIVEDI, MH, 2010, Effect of 11 September 2001 terrorist attacks

in the USA on suicide in areas surrounding the crash sites. The British Journal of Psychiatry: The Journal of Mental Science.

DIETZ, Klaus, HEESTERBEEK, J.A.P., 2002, Daniel Bernoulli's epidemiological model revisited, Mathematical Biosciences 180, 2 Elsevier Science Inc.

DORRUCCI, Maria, MINELLI, Giada, BOROS, Stefano, MANNO, Valerio, PRATI, Sabrina, BATTAGLINI, Marco, et. al. 2021, Excess Mortality in Italy During the COVID-19 Pandemic: Assessing the Differences Between the First and the Second Wave, Year 2020, Frontiers in Public Health, Volume 9, DOI: 10.3389/fpubh.2021.669209

DOWDLE, Erick, John, October 2008, Quarantine, Sony Pictures Releasing.

DURKHEIM, Emile, 2005, Suicide: A Study in Sociology, e Taylor & Francis e-Library.

EIKENBERRY, Steffen, MANCUSO, Marina, IBOI, Enahoro, PHAN, Tin, et al. 2020, To mask or not to mask: Modeling the potential for face mask use by the general public to curtail the COVID-19 pandemic, Infectious Disease Modelling, School of Mathematical and Statistical Sciences, Vol. 5.

GLASS, L.M., GLASS, R.J., 2008, Social contact networks for the spread of pandemic influenza in children and teenagers, BMC Public Health.

GLASS, Robert, J; GLASS Laura M., Beyeler Walter E, Min H. Jason, 2006, Targeted social distancing design for pandemic influenza, Emerging Infectious Diseases, Vol. 12, No. 11, November.

LENZER, Jeanne, 2006, Secret report surfaces showing that Pfizer was at fault in Nigerian drug tests, BMJ (Clinical research ed.) vol. 332

LEWIS, Michael, 2021, The Premonition: A Pandemic Story, UK: Penguin Books.

PETERSEN, Wolfgang, March 1995, Outbreak, Warner Bros. Entertainment Inc.

PLOS, Speaking of Medicine and Health, 2011, Failed vaccine campaigns are a global issue, URL: https://speakingofmedicine.plos.org/2011/09/12/failed-vaccine-campaigns-are-a-global-issue/#_ENREF_1

PRASSO, Sheridan, 2020, China's Divorce Spike Is a Warning to Rest of Locked-Down World, URL: https://www.bloomberg.com/news/articles/2020-03-31/divorces-spike-in-china-after-coronavirus-quarantines

RADELOFF, D, PAPSDORF, R, UHLIG, K, VASILACHE, A, PUTNAM, K, von KLITZING, K, 2021, Trends in suicide rates during the COVID-19pandemic restrictions in a major German city, Cambridge University Press, Epidemiology and Psychiatric Sciences 30.

Reuters, COVID-19 Global tracker, URL: https://graphics.reuters.com/world-coronavirus-tracker-and-maps/

SHEYNIN, O.B., 1977, D. Bernoulli's work on probability, in: M. Kendall, R.L. Plackett (Eds.), Studies in the History of Statistics and Probability, vol. II, London.

SHULTS, Edward Trey, April 2017, It Comes at Night, A24.

SMITH, David, 2011, Pfizer pays out to Nigerian families of meningitis drug trial victims, URL: https://www.theguardian.com/world/2011/aug/11/pfizer-nigeria-meningitis-drug-compensation

SODERBERGH, Steven, September 2011, Contagion, Warner Bros. Pictures

Staff, Indy, 2015, Six Thomashefsky Patients Test Positive for Hepatitis, Santa Barbara Independent, URL: https://www.independent.com/2015/04/21/six-thomashefsky-patients-test-positive-hepatitis/

DOI: 10.53477/2668-6511-22-06

THE ROLE OF LAW ENFORCEMENT AND PUBLIC SAFETY FORCES FACING BIOLOGICAL THREAT

Iulian-Constantin MĂNĂILESCU,
Ph.D. Candidate, Public Order and National Security,
„Alexandru Ioan Cuza" Police Academy**,** Bucharest, Romania
E-mail: driulianmanailescu@yahoo.com

Abstract: *The COVID-19 pandemic has shown that both state structures and citizens have not been prepared to face up a biological threat. The hesitant way in which, at first, action was taken to limit the spread of the new virus led to the emergence of situations that changed the relationship between the state and the population. The trust of a part of the citizens in the state structures has been altered, especially because of the restrictions imposed to limit the spread of the virus. Those who are in direct contact with citizens and who apply these restrictions are the law enforcement and other forces protecting public order and safety. At present, the countries of the world are in a position to think over some strategy meant to restore the confidence of their population in these forces. This distrust, along with conspiracy theories, endangers national and regional security because it is the ground for the proliferation of populism and extremism. The paper presents the sticking points of the relationship between the citizen and the law enforcement and public safety forces that a strategy at the state and regional level should solve in order to restore a level of trust at which security is ensured.*

Keywords*: law enforcement; public safety; biological threat; trust; strategy.*

Introduction

Pandemics are primarily outbreaks of infectious diseases that are transmitted from one human being to another and spread around the world. Beyond the debilitating, sometimes fatal consequences for those affected, they have negative social, economic and political consequences. They tend to be more problematic when the pandemic is due to a new pathogen, the mortality and hospitalization rate is high and spreads rapidly. According to Lee Jong-Wook, former director-general of the World Health Organization (WHO), pandemics do not respect borders. (World Health Organization, 2005) They can therefore simultaneously threaten societies, political systems and economies.

In the 1990s, more attention than ever was paid to pandemics and the threat to national security. In 1995 the World Health Assembly (WHA) agreed to revise the International Health Regulation (IHR), the only international legal framework governing how the WHO and its member states respond to outbreaks of infectious diseases, on the grounds that a review was needed to take into account ”the threat posed by the international spread of new and recurring diseases.” (World Health Organization 1995, 8)

In 2005 IHR revisions were adopted as AMS Resolution 58.34. Article 2 provides that the object and scope of the Instrument is the prevention, protection, control and response to the international spread of diseases through proportionate public health actions with the risks they pose to public health." (World Health Organization 2005, 7) Since its enforcement in 2007, the signatory states have worked individually and together to develop their basic capacities within the new framework.

In the Report on the Safety and Security of Humanitarian Personnel and the Protection of United Nations Personnel, UN Secretary-General António Guterres stated that: "Global security has entered a phase of increasing and widespread disruption, characterised by an increased risk of civil unrest and a steady increase in instability around the world." (United Nations, 30 Octobre 2020). If we are to look at what is happening in many countries of the world, his apprehension has come true If, from an economic point of view, the situation seems to have a solution, in terms of security, the problems persist, especially in terms of citizens' trust in state institutions. The defeat of Donald Trump in the US presidential election last November and the relative inability of populists to make their voices heard on the health issue seem to testify to a new political cycle less promising for parties such as the National Rally (RN) in France, the Alternative für Deutschland (AfD) in Germany or the Lega in Italy.

In general, when beeing in opposition, right-wing populist forces struggle to occupy space, such as the German AFD, the Austrian Freedom Party (FPÖ) or the Batavi populists. In France, the RN does not seem to really benefit from the health crisis. If polls on voting intentions anticipate new records for Marine Le Pen, they must be read with the utmost caution, as the 2022 presidential term remains relatively distant and the electoral offer very uncertain (Cautrès, 2021). In Germany, these forces, following the September elections lost a significant number of seats this year.

In some European countries, populist formations already seem able to capitalize on concerns related to the health context, such as the recent appearance of Chega in Portugal or the Alliance for The Unity of Romanians (AUR) in Romania.

At the heart of the speeches of these formations are conspiracy theories about the COVID-19 pandemic. Mainly, they assert that the state, or the powerful states of the world, are in fact dictators who are using a disease that does not exist, in order to limit the freedoms of citizens. All measures taken to eliminate the pandemic: physical distancing, mask wearing or vaccination are considered measures to eliminate part of the population or turn citizens into slaves. Manifestations of physical disobedience are also encouraged, even those involving violence.

It is the law enforcement and public safety forces that are in direct contact with citizens in the application of the regulations governing restrictions. There are also those who must ensure the conduct of public events within the limits of the law. The policeman, regardless of state, is the one who imposes fines, for example. The anger of those who are followers of populist or conspiracy theories have a concrete person to show their anger at. Even if they are not followers of populists, some citizens end up feelings adverse towards law enforcement victimizing those who break the law and who are subject to tougher measures, especially in case of public meetings (the use of water cannons, for example).

Public order and national security are essential military and non-military capabilities of national security. An essential condition for them to remain of a standard that ensures a life democratic, it is necessary for citizens to have confidence in this type of authority. Such trust reduces the risk of accepting all sorts of populist, extremist and anarchist theories. If anti-state propaganda is prolific, present in all social networks, circulated by some media institutions, and this is not since the advent of the pandemic, the promotion of the role of law enforcement and public safety forces has been neglected in most of the countries of the world. In Romania, the situation is more dramatic, in schools the role of the policeman has been almost excluded from education. The new generations have refutations, rather, about the negative parts of the police, presented in the media, and nothing about how they should relate to this authority. Campaigns to explain how a democratic state works seem to be increasingly necessary.

If Sars COV-2 has found more types of vaccines, the treatments are increasingly yielding, the biological danger is that of non-compliance with restrictions amid the refusal to vaccinate. The forces of public order and safety, against a high background of distrust, are in a

situation never seen before. In the application of laws concerning the pandemic, the opposition comes, and is often organized by representatives of the legislative or judicial power. Specifically, they are not in a position to deal with violent manifestations of those who do not accept the restrictions, but they are encouraged by parliamentarians or, in some states, by members of governments, but their work ends up being destabilised by some court decisions. Thus, their role in a safe society comes to be equated with that of representatives of forces that seek to harm the fundamental rights and freedoms of people. This article emphasizes, in particular, what has happened in Romania since the establishment of the state of emergency in the context of the pandemic. Any risk to the national security of this country poses a risk to European security. Without the application of a strategy to combat any biological threat, in which the main factor is held, in direct contact with the population of a country, the forces of public order and safety, the biological agent, regardless of its nature, or what it is sick, human or animal, spreads uncontrollably, affecting, as I said, security in all its dimensions. eventually destroying the democratic essence of a state.

1. Police response during the COVID-19 pandemic

Police services around the world are facing unprecedented challenges due to the COVID-19 pandemic. These challenges are related to the complexity and scale of the activities that the police are called to carry out and the changing nature of the role of the police during the pandemic. Although health workers are at the forefront, the police should be involved at every stage and the main interface with the population to answer citizens' questions and respond to their requests. Police services are overwhelmed by additional missions due to urgency: apps in public health orders, including quarantine or travel restrictions; securing health facilities, controlling the movements of large groups of people, helping to manage mass deaths, the protection of national stocks of vaccines or other medicines and the mission of informing the public and communicating risks. Coordinating the response is not spontaneous, as the police may have previously worked with most of the agencies through which the pandemic response plan is coordinated, including public health; medical workers and other basic bodies, such as telecommunications, electricity and water entities. In addition, the use of the military to enforce the application of emergency measures in many countries poses additional inssues in the relationship between the police and the Army Force becouse of some gaps in areas of competence and responsibility.

In the case of emergency situations, or those involving a security threat, the role of the police is well defined. The same is not the case with a pandemic because, in addition, complex situations arise that do not allow the definition of precise police roles in managing the situation.

Generally speaking, it is mentioned that more than the usual functions, the police have a Role in supporting the fight against the disease of and protect people from contamination.

The role of the police is also evolving to the extent that the context of the pandemic is changing and the needs of the population and the government are evolving. For example, courts may prioritise certain cases over others, depending on the situation, which will affect police decisions on crimes, prosecution and other cases for investigation.

Police staff requirements and organizational capabilities may also change during the pandemic, as they and their families may be affected by the deasese it self, at least in the same proportion as the rest of the population.

It is therefore extremely important to plan the police response to COVID-19 to deal with the evolving issues of preparedness, intervention and recovery after the pandemic. The importance of planning also lies in the reputational risks that the police may face during the

response to the pandemic, knowing that the measures taken today would have an impact on the future relationship between the police and the population after the biological crisis.

2. Trust in police influenced by the pandemic

2.1. France

In the case of France, trust in the police, as measured annually by the CEVIPOF Trust Barometer, fluctuated between 63% and 69% between 2009 and 2014. In 2015, attacks against the satirical newspaper Charlie Hebdo and Hyper Cacher were at the origin of an 11-point return of confidence, bringing this rate to the unprecedented level of 80%. However, within six years, French confidence in the police fell by 11 points, until the total cancellation of the capital acquired during the 2015 attacks. This erosion of the increased trust granted by the French during the attacks seems strange in the case of the police while the army, credited with a trust rating of 83% in February 2015 (a 7-point rebound from December 2014), benefited with a trust rating of 77% in February 2021. (Farde and Labarussiat 2021, 3)

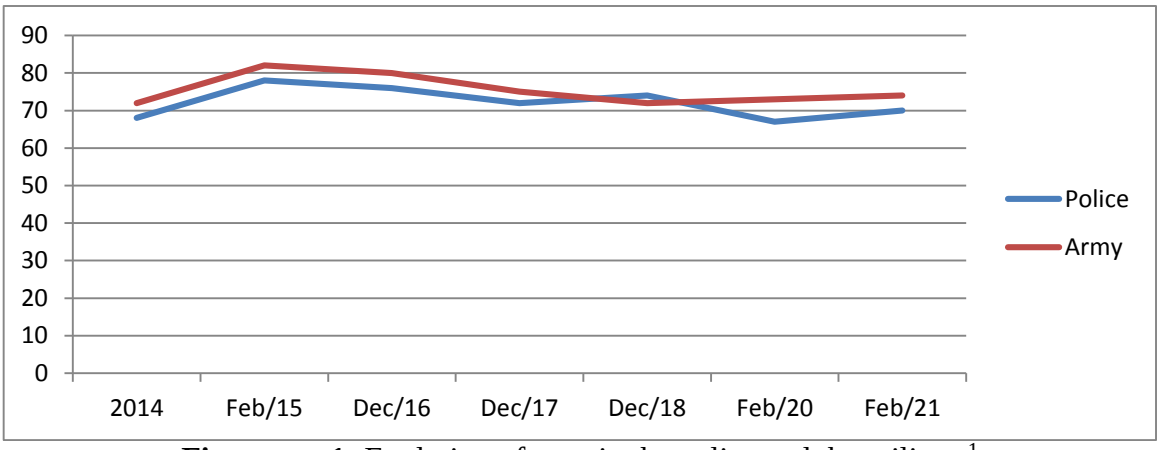

Figure no. 1: Evolution of trust in the police and the military[1]

However, in France, in 2020, the year when most restrictions were imposed, trust in the police had a slight climb. In 2020, due to restrictions, the number of demonstrations declined and police-demonstrators clashes were fewer. If in the case of the terrorist attack on Charlie Hebdo, the intervention of the police was considered beneficial, in 2020 and the first month of 2021, the police intervention in the case of the pandemic did not have the same good perception. As there were no large-scale confrontations like those in 2018, 2019, in which the „yellow vests" almost started a war with law enforcement, forces the citizens' dissatisfaction did not spill over to the police.

2.2. Federal Republic of Germany

Most Germans trust doctors, the police, universities and the Federal Constitutional Court. This is the result of a survey published in Cologne by the Forsa Institute for rtl/nTV trend barometer. „Four-fifths of citizens each trust the police and the Federal Constitutional Court (78 percent)". (Forsa poll: Doctors and police enjoy great confidence 2021)

More than 4,000 citizens were surveyed at the beginning of the year. A year earlier, most socially relevant institutions had performed worse. In May - during the coronavirus pandemic - trust returned to most institutions and has remained at a high level since then.

[1] Source: Data obtained from the survey Le décrochage des 18-24 ans, Note de recherche Le Baromètre de la confiance politique / Vague 12, March 2021,

In the case of Germany, in addition to the existence of a consolidated democracy, the state institutions had a good communication with the citizens and explained each of the regulations established at federal level and in each land, with how to apply them and the duties of each authority involved.

2.2. Romania

As far as Romania is concerned, the General Police Inspectorate, in collaboration with the National Institute of Statistics, conducted the study „Public Safety Survey" for several years, respectively 2015, 2016 and 2017. The investigation also concerned the trust in the police as a governmental institution, and the measured indicator was the degree of trust in the police and other institutions on duty in the sphere of public safetyand the question applied was: How much trust do you have in ...? (Ancheta siguranței publice 2015, 2016, 2017).

Table no. 1: Trust in institutions[2]

2015		2016	2017
Gendarmerie	71,3%	75,3%	77,1%
Police	68,3%	72,1%	75,1%
Border police	65%	69,3%	71,7%
Local police	64,7%	66,7%	68,1%

As seen in the table above, the trust in the police was in a continuous climb. Trust has been steadily growing for all law enforcement and public safety institutions.

The same studies have established the degree of satisfaction of the citizens, during the same period, in the work of the police.

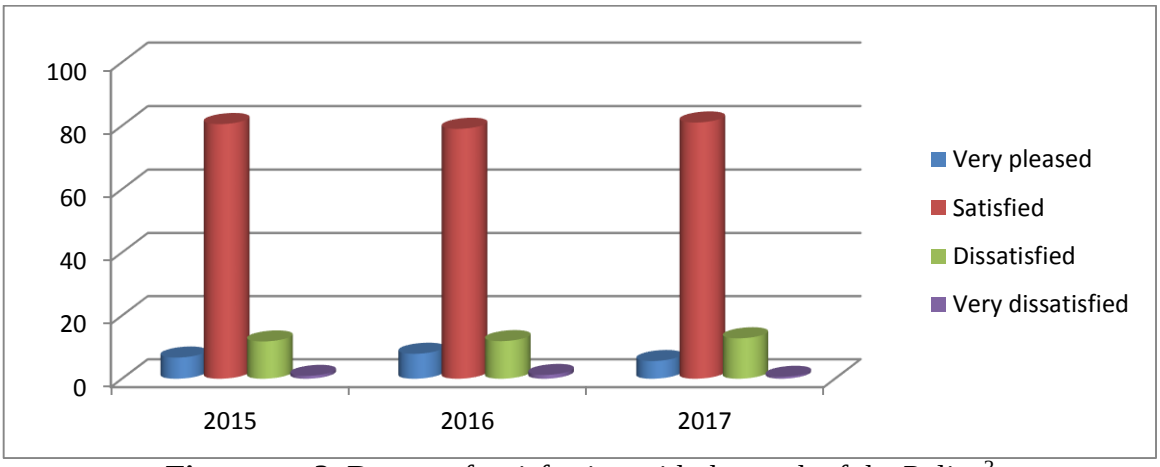

Figure no. 2: Degree of satisfaction with the work of the Police[3]

Even though the trust in the institutions of public order and safety has increased, the degree of satisfaction with the work of these institutions has remained approximately constant. To the satisfied answer, the variation was about one percent.

As has been observed during the COVID-19 pandemic, the authority of the police has played an important role, and as will be seen in the article, this authority may be questioned.

[2] A.N.: Data obtained from Ancheta siguranței publice, 2015, Ancheta siguranței publice, 2016, Ancheta siguranței publice, 2017.
[3] A.N.: Data obtained from Ancheta siguranței publice, 2015, Ancheta siguranței publice, 2017, Ancheta siguranței publice, 2017.

What's interesting is what level of trust this trust was at during the pandemic years. Unfortunately, the only relevant studies exist since 2015, 2016 and 2017.

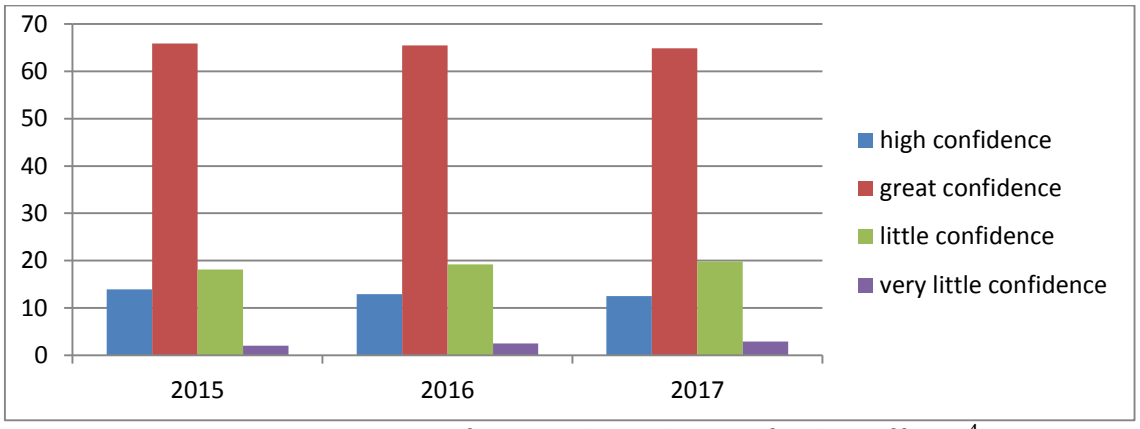

Figure no. 3: Degree of trust in the authority of police officers[4]

As seen in the chart above, the trust in the authority of the police was at a high and steady degree.

For the period before the pandemic, the study „Top trust in domestic and international institutions. The Army, the Church and the Gendarmerie on the first places / NATO and the European Parliament in terms of external institutions"[5] , carried out at the command of the Konrad Adenauer Foundation between 5 and 13 March 2019, showed a constant trust in the institutions that ensure national security. (G 4 Media.ro 2019)

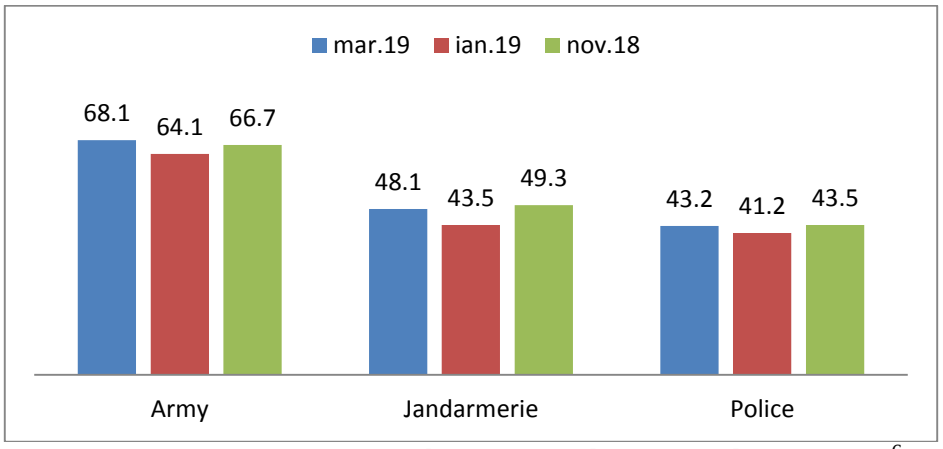

Figure no. 4: Trust in national security authorities and institutions[6]

Of all the national security authorities, the police recorded the lowest degree of trust.

In March, 2020, when in Romania by presidential decree it entered into a state of emergency. The legislation provided for the restriction of certain rights and freedoms, such as:

a) free movement;
b) the right to intimate, family and private life;

[4] Data obtained from Ancheta siguranței publice, 2015, Ancheta siguranței publice, 2017, Ancheta siguranței publice, 2017.
[5] Article 2, DECREE No. 195 of March 16, 2020 on the establishment of the state of emergency on the territory of Romania, published in the Official Gazette no. no. 212 of 16 March 2020
[6] Data obtained from the INSCOP Survey: Top trust in domestic and international institutions. The Army, the Church and the Gendarmerie on the first places / NATO and the European Parliament in terms of external institutions, March 22, 2019.

c) inviolability of the home;
d) the right to learn;
e) (e) freedom of assembly;
f) the right to private property;
g) the right to strike;
h) economic freedom.[7]

As will be seen in the following examples, these restrictions were met with violent manifestations towards the police, the first authority with responsibility for compliance with the norm.

The survey conducted by INSCOP: „How much confidence do Romanians have in the professions most exposed to risks in the context of the spread of the coronavirus epidemic" showed what was the level of trust in the police in March 2020. (INSCOP 2020).

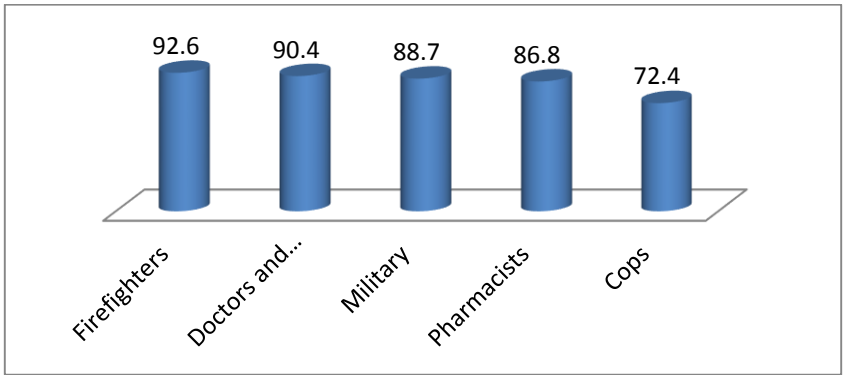

Figure no. 5: Romanians' trust in professions at risk during the pandemic[8]

As seen in the graph above, the police showed the lowest degree of trust, which announced the existence of a problem with the policeman-citizen relationship.

Three months later, the Romanian Institute for Evaluation and Strategy – IRES conducted the study: "2020 – Elections in pandemic" which evaluated the citizens' trust in the state institutions. (Sondaj realizat în iulie 2020)

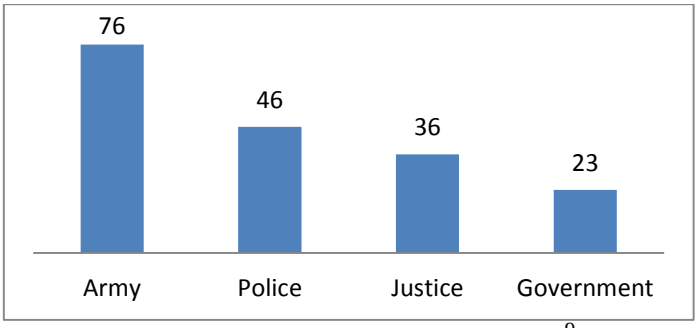

Figure no. 6: Trust in institutions[9]

The results are relevant because they provide a differentiation of trust in the police from trust in the military. In March 2020 this difference stood at about 16 percent, in just three

[7] A.N.: Article 2, DECREE no. 195 of March 16, 2020 regarding the establishment of the state of emergency on the Romanian territory, published in the Official Gazette no. 212 of 16 March 2020.
[8] A.N.: Data obtained from the INSCOP survey:"How much confidence do Romanians have in the professions most exposed to risks in the context of the spread of the coronavirus epidemic", march 2020.
[9] A.N.: Data obtained from the IRES survey: „2020 - Elections in pandemic", July 2020.

months, in June of the same year, the percentage climbed to 30%. This shows that the imposition of restrictions has led to a decrease in trust in the police.

The reluctance towards the measures imposed by the state of emergency, especially those that referred to the limitation of the right of movement, was manifested by aggression towards the policemen. Thus, in April 2020, in Rahova several people who organized a party with music in the middle of the street, threw stones and various objects at the policemen who arrived at the scene to restore public order and safety. Not only was the authority conferred by the status of a policeman not taken into account, but it required the intervention of other law enforcement who had to resort to gunfire. (DIGI 24 2020) This type of incident has been repeated in several places in the country, such as Galați.

Throughout the state of emergency and the alert period, there were verbal altercations between citizens and policemen regarding the wearing of a mask.

The authority of the policemen and the trust in them is questioned by the entry into the Romanian Parliament of the first anti-system and populist party, the Alliance for the Unity of the Romanians (AUR). The speech of the new lawmakers is calling into question the very essence of the work of the policemen in the pandemic. The state becomes, according to the propaganda made by this party, the enemy of the people who, through the restrictions imposed, want to turn the citizens into slaves, and even kill them by vaccination.

The support of all sorts of conspiracy theories from the parliament rostrum, the attacks, often furious at state institutions and authorities, turn the policeman from a defender of the law into a criminal. Not only is his authority thus eliminated, but his very physical integrity is endangered. When the one who has to restore public order and safety loses his authority, in the midst of the hybrid information war, national security is put at risk. In such a situation, security is attacked frontally from at least two sides.

Conclusions

In the situation of the COVID-19 pandemic, security is under attack from at least two sides. First of all, the attack is directed at national health, the non-observance of restrictions, the small number of vaccinated people end up bringing to its knees the health system that, nowhere in the world has been built to cope with such a large number of sick people as Sars-COV2 does. Second, public order and national security are under attack. The implications of the pandemic lead to a state of tension and revolt among citizens, whose rights and freedoms are restricted. The serious thing is that this attack can no longer be effectively countered by law enforcement and public safety forces, because the degree of trust in their work and authority decreases. However, as we have seen in the case of Germany, this kind of trust has remained high despite the pandemic. In addition to the history and socio-psychological typology of the citizens of this country, behind this trust lies a strategy, over several years, of how the state promotes and explains its actions. The role and duties of police officers are well understood by the average citizen.

France has the peculiarity, against the background of left-wing ideologies, of having, frequently, demonstrations and strikes. In the case of the "yellow vests" we can say that the actions of the state authorities and institutions have not been sufficiently well explained and that, although the demonstrators destroy and manifest themselves violently, the response with the same measure of the authorities is reinterpreted as dictatorial actions on the part of the state. Populist, anti-system political forces are also there against the measures taken to combat the COVID-19 pandemic, but their share will be about after next year's elections. In the June 2021 regional elections, the National Assembly, the far-right party of France's Marine Le Pen, failed to win in any region.

In Romania, at least in the case of the Police as a public order and safety authority, confidence in its activity and authority is decreasing. AUR, a political party that opposes the measures to combat the pandemic and which is against the current state structure, according to the latest polls is active both in the parliament's rostrum, but also in the public, physical and online environment, with messages of physical, antivaccine disobedience. In this situation, it is all the more necessary to carry out studies by identifying citizens' dissatisfaction and expectations towards police officers, establishing key points for a promotion of their activity and restoring the level of trust.

Restoring the citizen's trust in law enforcement and public safety involves a state-wide strategy. At EU level, the general framework of this strategy must be established: the causes that lead to the weakening of trust, the actors that can bring about this trust. Each state, the EU member would have to set its own strategy. A main point of this strategy, at the level of the general framework, is necessary to: the regulation as clear and appropriate as possible to the situations possible, in the normative, by each Member State of all the actions of the police officers involving, any type of citizen-police relationship.

We have stated in the above lines that the role of the police in the event of a pandemic is far from defined. But, in the last almost 2 years, they have outlined the role of law enforcement and public safety forces in real pandemic situations. The pandemic started in 2020 has created the possibility of including in national security strategies the definition of the role of the police, in the event of a biological threat.

BIBLIOGRAPHY:

***, Article 2, DECREE no. 195 of March 16, 2020 regarding the establishment of the state of emergency on the Romanian territory, published in the Official Gazette no. 212 of 16 March 2020.

***, DIGI 24. 2020. "Bătaie cu pietre în plină stradă, în București. Polițiștii au tras și focuri de armă. 37 de persoane duse la audieri." 19.04.2020, URL: https://www.digi24.ro/stiri/actualitate/bataie-cu-pietre-in-plina-strada-in-bucuresti-politistii-au-tras-si-focuri-de-arma-1294508

***, DIGI 24,2021. "Partidele lui Macron și Le Pen suferă înfrângeri categorice la alegerile regionale din Franța. Record de absenteism." 27.06.2021, URL: https://www.digi24.ro/stiri/externe/partidele-lui-macron-si-le-pen-sufera-infrangeri-categorice-la-aleg

***, Forsa-Umfrage. 2021. "Ärzte und Polizei genießen großes Vertrauen. Forsa-Umfrage". Evanghelisch.de, 11.01.2021, URL: https://www.evangelisch.de/inhalte/181070/11-01-2021/forsa-umfrage-aerzte-und-polizei-geniessen-grosses-vertrauen

***, Fundația Viață și Lumină, Asociația Centrul pentru Inovare Publică, Institutul Român pentru Evaluare și Strategie – IRES. 2020. "*2020-Alegeri în pandemie"*, sondaj, Institutul Român pentru Evaluare și Strategie, 2020.

***, G4 Media.ro. 2019. "Topul încrederii în instituții interne și internaționale. Armata, Biserica și Jandarmeria pe primele locuri/ NATO și Parlamentul European la capitolul instituții externe." *G4 Media.ro*, 22 march 2019: https://www.g4media.ro/sond

***, INSCOP Research. 2020. "Câtă încredere au românii în profesiile cele mai expuse riscurilor în contextul răspândirii epidemiei de coronavirus" URL: https://www.inscop.ro/graficul-saptamanii-cata-incredere-au-romanii-in-profesiile-cele-mai-expuse-riscurilor-in-contextul-raspandirii-epidemiei-de-coronavirus/ (sondaj INSCOP martie 2020)

***, Institutul de Cercetare și Prevenire a Criminalității. 2016. "Ancheta siguranței publice, 2015", https://www.politiaromana.ro/files/pages_files/ancheta_sigurantei_publice_2015.pd, 2016.

***, Institutul de Cercetare și Prevenire a Criminalității. 2017. "*Ancheta siguranței publice, 2017".* https://www.politiaromana.ro/files/pages_files/ancheta_sigurantei_publice_2016.pdf, 2018.

***, Institutul de Cercetare și Prevenire a Criminalității. 2018. "*Ancheta siguranței publice, 2017".* https://www.politiaromana.ro/files/pages_files/ancheta_sigurantei_publice_2017.pdf, 2018.

***, United Nations. 2020. "COVID-19 for global security: heightened instability and increased threats to United Nations staff, ORG/1711." URL: https://www.un.org/press/en/2020/org1711.doc.htm

***, World Health Organization. 2005. "The World Health Assembly adopts new international health regulations: the new rules govern the national and international response to outbreaks". URL: https://apps.who.int/mediacentre/news/releases/2005/pr_wha03/en/index.html

***, World Health Organization. 1995. "Review and Update of International Health Regulations", WHA48.7, World Health Assembly 48, URL: https://apps.who.int/iris/bitstream/handle/10665/178296/WHA48_1995-REC-1_eng.pdf?sequence=1, 1995.

***, World Health Organization. 2005. "Review of International Health Regulations", WHA58.3, World Health Assembly 58. URL: https://www.who.int/ipcs/publications/wha/ihr_resolution.pdf, 2005.

CAUTRÈS, Bruno. 2021. "La confiance des Français à l'épreuve de la crise." *Institut Montaigne*, 25 february 2021 URL: https://www.institutmontaigne.org/blog/la-confiance-des-francais-lepreuve-de-la-crise

FARDE, Guillaume and LABARUSSIAT, Floriane, 2021. "La confiance police-population en 2021: Le décrochage des 18-24 ans, Note de recherche Le Baromètre de la confiance politique". *Vague*, 12 march 2021: 1-11.

LABARUSSIAT, Guillaume and Floriane, FARDE. 2021. "La confiance police-population EN." *Sciense Pro*, 2021: 1-10.

DOI: 10.53477/2668-6511-22-07

TERROR ATTACKS AGAINST AFRICAN HEALTH FACILITIES

János BESENYŐ, Ph.D.
Associated Professor, Obuda University, Budapest, Hungary.
E-mail: besenyo.janos@gmail.com

Abstract: *The article is about the attacks on health facilities including hospitals, medical staff and security inside the healthcare institutions. The author first goes on to present a short introduction about the general knowledge concerning the situation of the terrorist assaults on the hospitals and the medical staff. He divides the text into several chapters, which try to comprehend the most important sides of the attacks ont he healthcare institutions. First, he starts with armed assaults on hospitals and health workers, where he describes the dangers the terrorists pose against the institutions and the personnel in them. Then he goes on to talk about the attacks by radicalized medical staff against their own personnel and patients, which presents a serious problem for the security officers. He continues with attacks by explosions, hostage taking and cyber attacks on medical facilities. At the end, the author concludes the article by giving some advises for the international community how to resolve these problems.*

Keywords: *healthcare facilities; terrorism; radicals; medical staff; explosions; hostage taking; cyber attacks.*

Altogether, there was 216 terrorist attacks against
health facilities, health workers, in Africa 1974-2019.

Introduction

First and foremost, it is important to define the brief meaning of terrorism before one jump into the ocean of evaluating violent acts against healthcare facilities. There are some reliable sources which give a definition of the concept. According to Britannica, terrorism is "*the calculated use of violence to create a general climate of fear in a population and thereby bring about a particular political objective.*" (Jenkins, 2021). Other sources give different examples for the phenomenon; for example: "*A policy intended to strike with terror those against whom it is adopted; the employment of methods of intimidation…*" (Oxford English Dictionary, 1989). Finally, there is a short but useful definition of terrorism: *"(threats of) violent action for political purposes*" (Cambridge English Dictionary, 2021). It is also necessary to enlist the organizations which participate in such murderous acts of violence on the continent regionally. In North Africa there are several active terrorist cells. The most important ones operate in Algeria, Tunisia, Libya and Egypt. These are the Al Qaeda in the Islamic Maghreb (AQIM), Shabab al Tawhid (or Ansar al Sharia Tunisia (AST)), Okba ibn Nafaa Brigade (also Tunisia), Ansar al-Sharia Libya – Benghazi, Ansar al-Sharia Libya – Derna and Ansar Beit al Maqdis (ABM) in Egypt. In West Africa, in the Sahel region there are several other terrorist organizations in Mali, Burkina Faso, and Nigeria. The notable ones are Ansaroul Islam, Jama'at Nusrat al Islam wal Muslimin (JNIM), with its AQIM affiliates: The Sahara Emirate branch of AQIM, al-Mourabitoun, Ansar Dine, Macina Liberation Front (FLM) and another cell, the Movement for Unity and Jihad in West Africa (MUJAO) as well as the Islamic State in the Greater Sahara (ISGS). One of the most brutal organizations is the Nigerian Boko Haram and

along it there is another cell in the country called Islamic State West Africa. In East Africa there are also terrorist groups, including the infamous Al-Shabaab and the Islamic State in Somalia (ISS). In Kenya there are some organizations as well, for example the Al Hijra group, the Al Muhajiroun and the Jahba East Africa (Africa Center for Strategic Studies, 2017).

The terrorists of the ISIL (Islamic State of Iraq and the Levant-Libya) and Al-Qaeda cells carry out a lot of attacks on innocent health institutions and health workers in many countries in Africa (Warner and Hulme, *CTCSentinel*, 21–28). One of the most common targets are the hospitals which are the so-called "soft targets". Between 1974[1] and 2019 there were several terrorist attacks, which were not committed mainly against health personnel, but rather against health facilities that are an easy target for the radicals. These comprehend 24 countries, where 520 people died. The first attack was carried out in Ethiopia in 27 May 1971. The perpetrator was the Eritrean Liberation Front, which is hostile to Ethiopia (Newton 2002, 90). There was another attack against the country in 1978, which was not followed by further incidents until 1989. These atrocities were only the beginning of the terrorist activity that has perplexed the continent. Their timing was not incidental since the cold war was at its height. The terrorist had many affiliations, they came from Ansar al-Sharia, AQIM, MUJAO and several other organizations that devastated the continent at the time. The hospitals weren't protected very well by security forces; they were targeted a lot of times by the Muslim radicals who used a wide range of methods against these buildings. The terrorists regrouped according to ethnic and national affiliations (Gofas 2012, 17-32). They were functioning by local customs (Neumann, 2009, 18-19). The terrorist groups often made pacts with their governments to make it easier to commit suicide bombings or other terrorist activities. One of the examples is the Eritrean Liberation Front (Iyob 1997, 47). The movement and its affiliates often committed terrorist attacks against hospitals and other health departments. The aforementioned attacks were usual mainly until the 2010s. There were lot of methods which the radicals applied against the government forces and the health personnel in the hospitals, and these were usually targeted against these health facilities.

After 2010 the situation has changed: these organizations became international. There were numerous groups that committed terrorist acts on the continent. For example, it is possible to mention the Al-Gamaat Al-Islamiyya, which is an Egyptian terrorist group. It committed radical activities in Europe and in the Middle East as well. The other terrorist cell is the infamous Al-Qaeda, which has perpetrated several attacks on innocent civilians and government security personnel in Afghanistan, the Middle East and in our case in Africa as well (Hamzawy and Grebowski, Carnegie Papers, 2010, 1-19 and Neumann 2009, 18-19 and Rabasa, Chalk, Cragin, Daly and Gregg, Rand Corporation, 2002). The Al-Qaeda is very active in the region, it has a lot of affiliate groups and has interconnections with other terrorist organizations like ISIS and its relatives.

In recent times these islamist groups have changed as they have become much more fundamentalist and they started to be organized by radical thoughts. Their motivation was based on the destruction of the African and Western society (Field 2009, 198), and on the establishment of the Islamic Califate. They became active internationally, even in Europe and in the Middle East and they wanted to create a society that would be based on the sharia law and on islamist values, that disregard women and doesn't take into consideration the rights of the civilians and the population. These terrorist organizations were organized based on deeply fundamentalist views, they followed radical islam and they even resorted to violent activities against the health personnel and others. They wanted to destroy the international community, the nations and the global system in order to establish their Islamic state and they were willing to go far to achieve their goals.

[1] A.N.: Prior to 1974, I have found no terrorist attack on the African continent targeting a hospital or other health care facility.

Their system was comprised of a lot of groups, they could have been called an umbrella organization, which targeted the international Muslim community. They committed several terrorist acts, and their activity in Africa was emphasized and got more attention from the international community (e.g. suicide bombings). For example, Al-Qaeda perpetrated terrorist attacks against health personnel and hospitals (Roggio, Long War Journal, 2011), which received more concern from the European states and the global world. The attacks against health personnel was rare before 2011, but from then on it flourished and suicide bombings became widespread across the Muslim world, especially in the Middle East and in Africa. There were African radical organizations as well which committed terrorist acts against innocent people, such as Boko Haram, which is mostly active in Nigeria. For example, they perpetrated suicide bombings in Maiduguri, Nigeria. The group is responsible for kidnappings and hostage situations as well, and it is intertwined with the population of the country thus it isn't easy to be controlled. Their targets are not only hostile Muslim groups or civilians, but Western, Christian people and institutions. For example, the Coptic community in Egypt is under constant threat and danger from the radicals, and they have committed several terrorist attacks against the group which constitutes only a minority of the Egyptian population (Tony Blair Institute for Global Change 2018). In fact, the fundamentalists aim to destroy the Western society and its institutions as well, so they constitute a real problem for the European community (Finucane 2018, 8-12).

1. Armed assaults on hospitals, health workers

This type of attack is one of the most frequent terrorist attacks in the region. The radicals use heavy weapons, mortars, light arms, grenades. Besides other terrorist organizations it is possible to mention the Seleka movement in the Central African Republic which use such arms (Mickolus 2016, 196) They not only use heavy and light weapons, but they commit terrorist acts with stabbing weapons, baseball bats and stones. One such country in which these attacks take place in the Democratic Republic of the Congo (reliefweb.int 2019). These armed assaults took place not only against hospitals, but ambulances as well, which are one of the favourite targets of the radicals.

1.1. Attacks with the target to kill specific groups

These types of attacks were committed against health personnel and patients of the hospitals, and they are mostly fatal. There are some examples which are worth mentioning, for example there was an assault on Fawzi Miknail (Mizell and Smith 2015, 189), an Egyptian healthcare official in Assiut in 22 July 1993, or another attack could be mentioned which was committed against an Italian sister in 4 September 2006 in Mogadishu, Somalia, in the S.O.S. Hospital (Shay 2010, 101). As it has been mentioned before the Islamic State targets the Coptic community (Mickolus 2016, 163), which is a Christian minority in Egypt. Along the personnel and the patients, the security guards, military officers and police officers were also attacked, one example was in Algeria, in Sidi Bel Abbes – on 3 August 1992 a police officer was killed (Terrorism Database). The terrorists use other methods, they disguise themselves as patient (S., J. and L. 2008, 224) this way they can easily enter the health facilities, which are therefore in greater danger from the radicals.

1.2. Attacks by explosions

This is the second most popular method of the terrorists to attack health institutions and personnel. They commit these assaults at parking lots, main entrances, at the ambulance entrances, or even inside the facility as well. They generally place the bombs in cars or trash cans, but they can also carry the explosives with them on suicide vests or in their luggage. It is

also a preferred method to throw grenades on buildings, or on the rooms of the health institutions. Several times they carry hidden explosives inside the building. Usually, they carry their bags inside the building, which is a dangerous method, because the security personnel rarely checks the bags of the people entering the building. Sometimes the radicals park cars loaded with bombs outside the hospitals, or they even use ambulances to hide their intentions. There are a lot of instances when this type of attacks happened, Egypt is one of the known places for such bombings (Global Terrorism Database 2013). In 24 October 2013, Boko Haram stole two ambulances from the General Sani Abacha Hospital in Damatura, Nigeria (Global Terrorism Database 2013). It happened also in Burkina Faso (Lyammouri, Sahel Memo 2019) and Niger (caert.org.dz 2019), as well as in Libya, on 12 June 2016: this recent attack was perpetrated by the Islamic State's militia, which stole an ambulance car. They went to the hospital of the Libyan Army on 12 June 2016 in the town of Sirte, which resulted in one fatality (Mickolus 2016, 176).

There were also suicide bombings which were common from the 2010s. They are perpetrated usually by cars. Sometimes the terrorists even dressed as women (Maruf and Joseph 2018, 140-141). The assaults are widespread among the terrorist cells: first, they commit suicide or other bombings against civilians or government officials, then when the health personnel and the ambulances arrive, they carry out a second attack, in which the doctors and the patients are killed. There are several examples in which these attacks happened: one of them was in Jos, Nigeria, where the Boko Haram bombed the Terminus Market. When the ambulances arrived, there was another explosion. 59 people have died (Global Terrorism Database). In 5 August 2019, in Egypt the Hasm organization (which is an affiliate of the Muslim Brotherhood) bombed the Cairo University Teaching Hospital, where 20 people died and 47 suffered injuries (Michaelson, The Guardian, 2019.

2. Involvement of medical staff in terrorist groups

There are instances when health personnel become radicalized, and they even enter terrorist groups (Aboul-Enein 2004, 18) which generally take advantage of the opportunity to train them. Several times they terrorist activities or suicide bombings against their own patients, which present a serious problem for the security of the hospitals (Mizell 2015, 234-235). They are perpetrated usually by the Islamic State, but ISIL does it usually as well (caert.org.dz 2019 and Amiga and Schuster Haaretz 2015). There are other organizations which are responsible for the training of the medical staff, for example GSPC (Botha 2008, 120), Al-Qaeda (Bloom 2017, 603-623 and Perper and Cina 2010, 145-147), Ansar al-Sharia (Turak Tunisia Live, 2014), Al-Shabab (Maruf and Joseph 2018, 70-71) and Boko Haram (Ewi, Salifu, ISS Policy Briefs, 2017). This is why the medical personnel must be frequently checked and the hospitals must be thoroughly searched to avoid such incidents (Fischbacher-Smith and Fischbaher-Smith 2013, 337-338).

3. Taking hostages, kidnapping hospital employees

Altogether there was 44 cases of kidnappings in Africa until 2019. Generally, the terrorists use firearms, and ask for ransom to return the hostages. However, there are a lot of instances when they are not given back, instead the radicals kill them without asking for any ransom. For example, in 1 March 2018, at the Rann refugee camp, Nigeria the Boko Haram killed 3 people and abducted 3 sisters. From the kidnapped persons 2 were publicly executed on September 2018. Several times they are released by ransom or in some instances the secret services free them. Another example is the ISIL organization, which also perpetrated an attack

against the Sirte army hospital in Libya. 22 doctors were taken hostage on March 2016 (refworld 2018).

4. Cyber attacks

The internet system of the hospitals is prone to cyber-attacks and they are very vulnerable, for this, hackers target these institutions (Berman, nationalinterest.org, 2019), who belong to radical groups.

The cyber-attack can have two goals:

1. To prevent the proper functioning of the internet system of the patients' care, which puts the civilians and the hospital staff at a risk (phe.gov 2017 and Shapira, Hammond and Cole 2008, 261-262).
2. The terrorists gather data about the patients, and with that they can blackmail the healthcare staff and the civilians who are vulnerable (Rosenberg, Jerusalem Post, 2019).

Virus attacks and code-stealings can be dangerous as well, as they can affect or disfunction the healthcare machinery in the hospitals or other medical facilities (H. and F. and M and L J 2017, 94-100). Recently the cyber-attacks became frequent (Landi, Healthcare Innovation, 2018). This is why the defence against viruses is so important in the healthcare facilities.

5. Effect of the Covid-19 and other diseases in Africa on terrorism

To understand better the security situation concerning the attacks on health facilities, it is important to take notice of the recent events concerning the Covid-19 situation that has increased global insecurity in the world.

In overall, the cases of Coronavirus on the continent have been decreasing in the week between 4-10 October 2021 examined by the World Health Organization (WHO). The countries show a decisive reduction of Covid-19 cases concerning Africa. In general, in the abovementioned week there were 25,044 Coronavirus-infections in the region, while a week before the number was 44,212. This means a 43,4% diminution in the diseases in relation with the virus. The most infected countries of the region in this week were Ethiopia (5,807 persons), South Africa (5,723 persons), Angola (2,435 persons) and Nigeria (1,558 persons). These states account for the most infected areas of the continent in which the disease left a mark. However, the rate of illness in Africa is considered by WHO the smallest one among the other continents (3,6% of the worldwide epidemics). The numbers speak for themselves: in Africa there were 8.4 million illnesses caused by Covid-19 with 214,480 fatalities. This is negligible compared to other regions and continents of the world (World Health Organization, 2021).

Not only was Coronavirus the main problem for the African community, as other diseases have spread that affected the security of the countries. Notably the Ebola Virus, which caused several outbreaks in West Africa (Guinea, Liberia, Sierra Leone. Mali, Nigeria, Senegal) between 2014-16 (CDC, 2019) and in August 2021 (Cote d'Ivoire, Guinea) there was another case of a detected infection (WHO, 2021). West Nile Virus is also a terrible source of insecurity, as in the 2000s there were several cases reported of WNV outbreaks in North Africa (Morocco, Tunisia, Algeria, Egypt) and in Guinea, Ghana, Gabon and South Africa (Sayed-Ahmed, 2016, 102).

However, the biggest problem concerning health facilities is that these outbreaks will give the opportunity for the abovementioned terrorist organizations like AQIM and ISIS to exploit the ongoing health and food crisis and the inability of governments to act against the weakness of their domestic defence capabilities. Hospitals and health facilities that are not well-equipped are struggling to get a grip on the handling of the Coronavirus outbreak and other kind

of diseases, thus it is easy to see the inherent dangers that these infections pose to the spread of terrorism on the continent (Coleman, J.D., 2020).

Conclusion

In recent years the attacks against hospitals and healthcare facilities, as well as against medical facilities have multiplied. African militants, radicals who arrive from the Middle East and other foreign countries to the continent want to establish the islamic state They want to convert the Christians and subjugate the hostile muslim groups or the civilians in order to create a fundamental Islamic world on the continent and install the islamic law (the sharia). The terror attacks against the hospitals constitute a clear problem for the governments and the security forces notwithstanding the security guards of the healthcare facilities. The main problem is that these institutions have a very weak defence system and the security guards are not prepared to prevent these kind of attacks on the medical facilities of the African countries. Therefore, these buildings and their personnel are very vulnerable and they are a favourite target of the terrorist cells and organizations.

According to these facts, it is possible that there will be more similar attacks on such institutions – suicide bombings, murders during hostage takings and cyber-attacks. To make the healthcare facilities more secure, there has to be some measurements taken which are the following:

1. to analyse the terrorist attacks committed until 2019 in Africa and to integrate the results into the security systems of the hospitals;
2. to check the security situation of the healthcare facilities;
3. to prepare emergency plans and protocols, which should be controlled generally by the state organizations and the security forces;
4. the examination and correction of the security systems;
5. establishment of an inner security system, which should check the personnel working in these institutions;
6. to prepare against cyber-attacks.

These steps would eradicate or lessen the possibility of further attacks, although the danger of the situation probably would remain.

BIBLIOGRAPHY:

ABOUL-Enein, YOUSSEF H.. 2004. Ayman Al-Zawahiri: The Ideologue of Modern Islamic Militancy. Alabama: USAF Counterproliferation Center, 18.

Africa Center for Strategic Studies. 2017. "Map of Africa's Militant Islamist Goups." URL: https://africacenter.org/spotlight/map-africa-militant-islamic-groups-april-2017/

AMIGA, Aimee and SCHUSTER, Ruth. 2015. Haaretz. "EU Report: ISIS Could Commit Chemical or Biological Terror Attack in West.". URL: https://www.haaretz.com/middle-east-news/isis/eu-isis-could-commit-chemical-biological-attack-in-west-1.5436111

BERMAN, Ilan. 2019. "Technology is Making Terrorists More Effective – And Harder to Thwart.". The National Interest. URL: https://nationalinterest.org/feature/technology-making-terrorists-more-effective%E2%80%94and-harder-thwart-45452

BLOOM, Mia. 2017. "Constructing Expertise: Terrorist Recruitment and "Talent Spotting" in the PIRA, Al Qaeda, and ISIS." Studies in Conflict & Terrorism 40 (7), 603-623, DOI: 10.1080/1057610X.2016.1237219.

BOB, Yonah Jeremy. 2018. ”Exclusive: Islamic cyber terrorists trying to target infrastructure.” The Jerusalem Post. URL: https://www.jpost.com/Arab-Israeli-Conflict/Exclusive-Islamic-cyber-terrorists-trying-to-target-infrastructure-562052

BOTHA, Anneli. June 2008. Terrorism in the Maghreb, The Transnationalisation of Domestic Terrorism. Johannesburg: Institute of Security Studies, 120.

Cambridge English Dictionary. 2021. ”Terrorism.” URL: https://dictionary.cambridge.org/dictionary/english/terrorism

Centers for Disease Control and Prevention. 2019. ”2014-2016 Ebola Outbreak in West Africa.” URL: https://www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/index.html

COLEMAN J.D., Julie. 2020. ”The Impact of Coronavirus on Terrorism in the Sahel.” International Centre for Counter-Terrorism – The Hague. URL: https://icct.nl/publication/the-impact-of-coronavirus-on-terrorism-in-the-sahel/

De CAUWER H., SOMVILLE F., SABBE M., MORTELMANS LJ. 2017. ”Hospitals: soft target for terrorism?”. Prehospital and Disaster Medicine. 32 (1): 94-100.

EVAN, T., LEVERETT, E., RUFFLE, S. J., COBURN A. W., BOURDEAU J., GUNARATNA R. and RALPH, D.. 2017. Cyber Terrorism: Assessment of the Threat to Insurance, University of Cambridge. URL: https://www.jbs.cam.ac.uk/fileadmin/user upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf

EWI, Martin and SALIFU, Uyo. February 2017. ”Money Talks: A Key Reason Youths Join Boko Haram.”. ISS Policy Briefs 98. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ISS_Africa-policybrief98.pdf

FIELD, Antony. 2009. “The ‘New Terrorism’: Revolution or Evolution?”. Political Studies Review, 7 (2): 198.

FINUCANE, David J. 2018. ”Unhealthy complacency: The vulnerability of US hospitals to direct terrorist attacks.” Journal of Healthcare Risk Management 37 (3): 8-12.

FISCHBACHER-SMITH D. and M. 2013. ”The vulnerability of public spaces: challenges for UK hospitals under the 'new' terrorist threat.” Public Management Review 15.

Global Terrorism Database. ”Boko Haram suicide attack at Terminus Market in Jos, Nigeria.” URL: https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201405200067

Global Terrorism Database. ”Terror attack on police guard before Sidi Bel Abbes Hospital.” URL: https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=199208080001

Global Terrorism Database. 2013. „An explosive in an ambulance detonated near Egyptian soldiers in Rafah, Egypt.” URL: https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201310240011

Global Terrorism Database. 2013. „Boko Haram attack against General Sani Abacha Specialist Hospital, Damatura.” URL: https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201310240037

GOFAS, Andreas. 2012. “'Old' vs. 'New' Terrorism: What's in a Name?”. Uluslararası İlişkiler 8 (32) (Winter): 17-32. URL: https://dergipark.org.tr/tr/download/article-file/540175

HAMZAWY, Amr; GREBOWSKI, Sarah. 2010. „From Violence to Moderation Al-Jama'a al-Islamiya and al-Jihad.". Carnegie Papers, No. 20 (April): 1-19. URL: https://carnegieendowment.org/files/Hamzawy-Grebowski-EN.pdf

Health Care Industry Cybersecurity Task Force. 2017. „Report on Improving Health Care Industry Cybersecurity." URL: https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

https://www.oed.com/oed2/00249602;jsessionid=A14CBC89A41317E966650528756F5841

IYOB, Ruth. 1997. The Eritrean Struggle for Independence: Domination, Resistance, Nationalism, 1941-1993. St. Louis: Cambridge University Press. 47.

JENKINS, John Philip. 2021. „Terrorism." Britannica. URL: https://www.britannica.com/topic/terrorism

LANDI, Heather. 2018. „Report: Ransomware Attacks Against Healthcare Orgs Increased 89 Percent in 2017." Healthcare Innovation. URL: https://www.hcinnovationgroup.com/cybersecurity/news/13029655/report-ransomware-attacks-against-healthcare-orgs-increased-89-percent-in-2017

LYAMMOURI, Rida. 2019. „Burkina Faso: February 2019 SITREP and Chronology of Violent Incidents Related to AlQaeda affiliates Jama'at Nusrat al-Islam wal Muslimeen (JNIM) and Ansaroul Islam, and Islamic State in the Greater Sahara (ISGS)." 2016-2019 Sahel MeMo LLC. URL: https://www.sahelmemo.com/wp-content/uploads/2019/03/Burkina-Faso-SITREP_February2019.pdf

MARUF, Harun, JOSEPH, Dan. 2018. Inside Al-Shabaab: The Secret History of Al-Qaeda's Most Powerful Ally. Bloomington: Indiana University Press.

MICHAELSON, Ruth. 2019. „Cairo car bomb kills at least 20 outside hospital." The Guardian. URL: https://www.theguardian.com/world/2019/aug/05/at-least-20-dead-and-47-injured-in-explosion-outside-cairo-hospital

MICKOLUS, Edward. 2016. Terrorism, 2013-2015: A Worldwide Chronology. Jefferson: McFarland.

MIZELL, Louis R. and Smith. 2015. E. Reed; Terrorism & The Medical Environment. Tactics, Targets& Trends.

NEUMANN, Peter R. 2009. Old and New Terrorism. Cambridge: Polity Press.

NEWTON, Michael. 2002. The Encyclopedia of Kidnappings. New York: Infobase Publishing, Infobase Publishing.

Oxford English Dictionary. 1989. „Terrorism."

PERPER, Joshua A. and CINA, Stephen J.. 2010. When Doctors Kill: Who, Why, and How. New York: Copernicus Books.

RABASA, Angel; CHALK, Peter; CRAGIN, Kim; DALY, Sara A.; GREGG, Heather S.. 2002. "Beyond al-Qaeda: The Outer Rings of the Terrorist Universe.". Part 2 Rand Corporation,. URL: https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG430.pdf

ROGGIO, Bill. 2011. "AQIM suicide bombers kill 4 in Algeria.". Long War Journal. URL: https://www.longwarjournal.org/archives/2011/07/aqim_suicide_bombers.php

ROSENBERG, Oz. 2019. ”Health technology: Are medical devices protected?”. Jerusalem Post. URL: https://www.jpost.com/Israel-News/Israel-health-technology-Are-medical-devices-protected-588405

S., SHAPIRA., J . HAMMOND and L. COLE. 2008. Essentials of Terror Medicine. Springer Science & Business Media, 224.

SAYED-AHMED, Mohamed. 2016. ”Incidence history of west Nile virus inA frica and middle east, with emphasis on Egypt: a review.” Journal of Dairy, Veterinary & Animal Research, no. 3: 101-104. URL: https://medcraveonline.com/JDVAR/JDVAR-03-00080.pdf

SHAY, Shaul. 2010. Somalia Between Jihad and Restoration. New Brunswwick: Transaction Publishers, 101.

Terrorism-bulletin. 2019. ”Africa Terrorism Bulletin, African Centre for the Study and Research on Terrorism.”. URL: http://caert.org.dz/Medi-review/Terrorism-bulletin/Bulletin-6.pdf

The Safeguarding Health Conflict Coalition. 2019. ”Impunity remains: Attacks on Health Care in 23 Countries in Conflict 2018.” URL: https://reliefweb.int/sites/reliefweb.int/files/resources/SHCC2019final.pdf

The Tony Blair Institute for Global Change. 2018. ”How Islamist Extremists Target Civilians”, URL: https://institute.global/sites/default/files/articles/How-Islamist-Extremists-Target-Civilians.pdf

TURAK, Natasha. 2014. “Medical Student Fatma Zouaghi, Alleged Ansar Al Sharia Member, Arrested.” Tunisia Live. URL: https://web.archive.org/web/20170623133134/http://www.tunisia-live.net/2014/10/15/medical-student-fatma-zouaghi-allegedansar-al-sharia-member-arrested

United States Department of State. 2018. ”Country Reports on Terrorism 2017 - Foreign Terrorist Organizations: Islamic State of Iraq and the Levant-Libya (ISIL-LIBYA).” URL: https://www.refworld.org/docid/5bcf1f40a.html

WARNER, Jason and HULME, Charlotte. 2018. ”The Islamic State in Africa: Estimating Fighter Numbers in Cells Across the Continent.” CTCSentinel 11 (7). URL: https://ctc.usma.edu/islamic-state-africa-estimating-fighter-numbers-cells-across-continent/

World Health Organization, Africa. 2021. ”West Africa COVID-19 deaths surge amid Ebola and other outbreaks.”. 19 August. URL: https://www.afro.who.int/news/west-africa-covid-19-deaths-surge-amid-ebola-and-other-outbreaks

World Health Organization. 2021. ”Weekly Bulletin on Outbreaks and other Emergencies.” 4-10 October. URL: https://apps.who.int/iris/bitstream/handle/10665/346225/OEW41-0410102021.pdf

DOI: 10.53477/2668-6511-22-08

"LAZARUS" THE NORTH KOREAN HACKER GROUP

Attila GULYÁS,
Lieutenant Colonel (Retired), Ph.D. Student,
Safety and Security Sciences Doctoral School, Obuda University, Budapest, Hungary.
E-mail: gulyas.attila@Ph.D.uni-obuda.hu

Abstract: *The Democratic People's Republic of Korea (DPRK) is famous for the poverty, destitution and backwardness, however in spite of these negative features it is among the most advanced cyber warfare countries. In the daily news quite often can be read about cyber-attacks against different states, media institutions or banks where the experts assume that the DPRK supported hacker group the "LAZARUS" is behind the attacks. According to the latest news the group in connection with stealing a big amount of crypto currency and money laundering got into the limelight. The state officially denies the existence of the group however cyber analysts and security experts found direct and circumstantial evidences that prove the connection between the North Korean state and the hacker group.*

Keywords: *North Korea; Lazarus; APT; Bluenoroff; cybercrime; hacker.*

Introduction

The dissolution of the socialist world order posed a big challenge for the economy of North Korea. It lost its supporters and markets, today China is the primary trading partner of North Korea. In spite of its advantageous geographical location, and its mineral resources the economy of the country is in ruins due to the decades of mismanagement, under-investment, resource misallocation, poor maintenance and corruption. Big part of the population is continuously malnourished and live in deep poverty. The government spends up to 24 percent of the GDP on the military and military industry. The North Korean army is one of the biggest armies in number on the world with its more than million personnel, but their equipment is obsolete. The most part of the military budget spent on the nuclear and the ballistic missile programs which are condemned by the international community, except Iran. The government blackmails the international community with its nuclear program to get food and other supports from abroad. Depending on its interests it follows the international calls, and treaties or breaks the agreements. The United States declared North Korea as a rogue state in 2001, and then introduced monetary, export-import sanctions together with the United Nations to curb the North Korean nuclear and ballistic missile programs (United States Department of State, 2019).

The socialist leadership elaborated two way-outs to solve this seemingly hopeless situation. The first one is to improve the pressure on the International community with the nuclear black mailing while the second is a new cyber strategy that helps protect their cyber security and provides them with the cutting-edge technologies, and last but not least financially supports their nuclear and ballistic missile programs. They realized that the countries with high computer network and Internet penetration are vulnerable to cyber-attacks and cyber espionage. They also recognized that the cyber warfare is very cost effective because with relatively low investment the gain is high (Bartlett 2020a). The last element of their cyber strategy is similar to Queen Elizabeth's invention in the sixteenth century called „strategic crime". As is well known the Queen encouraged her piratical „Sea Dogs" to fill up her treasury (Arquilla 2021, 4).

1. The North Korean cyber organizational and the technological bases

The cyber activity of North Korea is coordinated by the Chief of Staff of Korean People's Democratic Army, Reconnaissance General Bureau (RGB), and the Korean Workers Party (Center for Strategic & International Studies 2014). According to the United States the Reconnaissance General Bureau is responsible for the cyber-attacks (Cha, & Lewis 2014, 26) that is why the paper focuses on it after presenting the technological, and educational bases of North Korea.

1.1. Industrial and technological bases

North Korea started improving its cyber capabilities in the late eighties, but the real breakthrough was in the late nineties when established the College Computer Science at Kim Il-sung University, and the Ministry of Electric Power Industry. The party leadership declared that the science technology as one of the three pillars to achieve the status as a "strong and prosperous nation." (ROK Ministry of Unification 2015). North Korea has systemically improved its IT industry focused on the software development. This technology is a very important part of the education both middle and higher level. The country has its own hardware and semiconductor development and production as well. According to South Korean police estimation approximately ten thousand IT professionals as guest workers are employed in Shenyang and Dangdong, China where they have access to the cutting edge hardware and software technologies (Seok & Sang-ki 2008, 7).

The Korea Computer Center and the Pyongyang Informatics Center are the main cores of the software and hardware developments.

In the country there are four independent intranet networks. One of them is for the military and the others are for governmental purposes. All of them are under strict control and cyber protection.

Korea Computer Center (KCC)

The Center was established in 1990. It is responsible for the research and development, and the hardware, software production. It is also supervising the IT education at university level. The center has right to trade abroad, allegedly it has subsidiaries in Germany, China, and Syria. The Center takes part in cyber-attacks and it uses its subsidiaries as cover firms (Jun et al. 2015, 54). The main profiles of their software development are Linux based operational systems. They developed the "Red Star" operational system that is North Korea's first operational system and their significant exported software solution. The KCC has more than one thousand personnel of which more than one hundred have PhD (Jun et al. 2015, 54). The organization multiple times was blamed for cyber related crimes especially in connection with South Korea. In the late nineties its employees developed illegal game exploits to popular pc games which were actually spy software solutions and these exploits were sold under false flag (pretending Chinese) in South Korea (Seok-woo 2011).

Pyongyang Informatics Center (PIC)

The PIC was established in 1986, and is located in Kyungheung-Dong, Botonggang District, Pyongyang. The Center primarily focuses on software development. It has more than 500 personnel including 180 researchers of which 30 have PhDs. The employees of the PIC developed the "Changduk" word processing software and the Dangun Korean language processing software, both are widely used in North Korea. The PIC has subsidiaries in Japan and Singapore.

The PIC was the center of the Inter-Korean IT cooperation in the early 2000s as a part of the South Korean "Sunshine Policy" which was a fruitful cooperation until the North Korean torpedo attack against the ROK Cheonan ship in March 2010. As a result of the attack the South Korean government banned all inter- Korean trade, and investment.

According to their original plans they would have produced competitive software solutions and establish a Silicon Valley like area and a software developing center in Dandong (Seongwook 2009). During the years of the cooperation the South Korean partner carried out site visitations and they concluded that the North Korean programmers were highly skilled and well ahead of the South Korean counterparts in IT security (Seunghyun 2004).

1.2. Educational basis

One of the North Korean government's priorities is the establishment of the educational basis of the cyber warfare. In order to accomplish this aim at the higher level IT educational institutes they introduced the hacker training. According to defectors reports in May 2020 the military recruited more than 100 hackers from the top science and technology universities to manage its intranet networks and tactical planning systems. One of these universities is the Kim Chaek University of Technology. Another good example is the Mirim College where more than 100 hackers graduate every year. North Korean defector reported that the students study the MS Windows operating systems, learn how to create destructive computer viruses, and code in various computer languages.

1.3 Organizational basis

Reconnaissance General Bureau

The first report on the RGB published in 2009. Analyst Joseph Bermudez describes this new organization as a new intelligence unit built of numerous special units and intelligence organizations (Bermundez 2010). These units were involved into commando, intelligence, sabotage, radio reconnaissance, and different kinds of covert actions. Until 2010 the general cyber capabilities were dispersed among different organizations and governmental agencies.

This service is responsible for all intelligence collection and covert operations, including cyber related crimes. It established companies and joint venture companies in Asia in order to cover the illicit financial operations. The Bureau in this way it tries to cloak its illicit activities including its launder money operations (Bartlett 2020a).

The next section gives an overall picture of the cyber warfare involved units of the RGB. Unfortunately, the strict censorship and the closed society make hard to get authentic information on these units, we can only refer to the open sources. It is not uncommon in the North Korean way of conspiracy that they give different names to units which has nothing to do with their original functions. Today the North Korean government command more than 6000 cyber agents through the RGB's subunits across the world - one of them is the "LAZARUS" of which activity will be discussed later in details in this study (Bartlett 2020a). The theoretical organizational chart of the RGB is can be seen on the Figure no. 1.

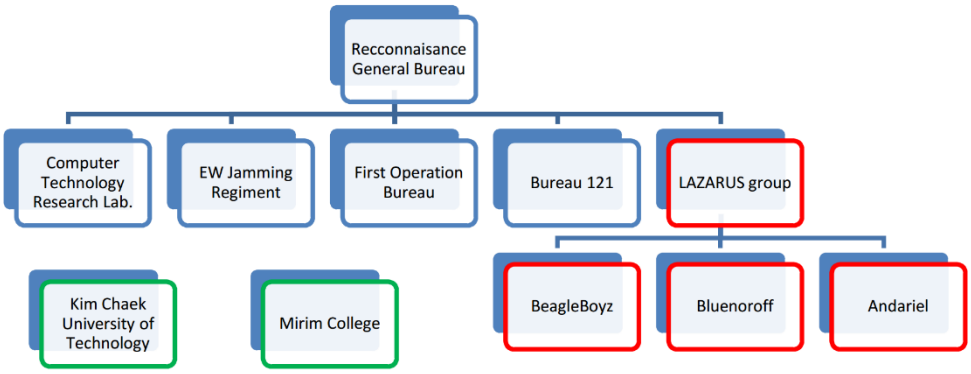

Figure no. 1: Identified North Korean Intelligence-led cyber organizations[1]

[1] Source: https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers, and complemented by the author

Bureau 121

The Bureau is the most important cyber unit of North Korea. Its mission includes offensive and defensive cyber operations, cyber espionage, network exploitation and cyber-crime. Different sources refer to it by different names such as Unit 121, Bureau 121 just to name a few. There is no available authentic open source information on its structure, or its personnel. According to North Korean defectors its new building complex was built in 2013 along with luxury apartments for the employees of the bureau in the northern part of Pyongyang (Jun et al. 2015, 41). The analysis of the satellite pictures didn't corroborate the information, but it didn't refute either, because it is not uncommon that the important objects are hidden under the surface.

Computer Technology Research Lab

It is a very interesting organization because this unit was identified that has hacking technics advanced enough to carry out attacks against South Korean financial institutes according to an open source report published in 2013 (Soonpyo Park 2013). The existence of this unit today is unknown, it may be disbanded, or merged into other units.

1st Operations Bureau or 414 Liaison Office or 128 Liaison Office

South Korean reports, and researches often refer to this organization as a major cyber unit under the RGB. In the Korean terminology the "liaison" word means support of the intelligence collection and commando actions against South Korea. This unit is responsible for the connection with the covert agents deployed abroad and it conducts surveillance on South Korean Law Enforcement Agencies (Lee 2014). Likely they develop cyber means for the cheaper and more effective information collection and for the connection with the agents. It is not unthinkable that the unit shares its cyber tools with other RGB units. Yet, it seems that major unit is an overstatement.

2. "LAZARUS" group

The LAZARUS group a cyber-criminal organization controlled by the North Korean intelligence Service (RGB). The group attacks governmental institutions, military, financial, manufacturing, publishing, media, telecommunication, entertainment and international shipping companies, educational institutions as well as critical infrastructures using means of cyber espionage, data theft, monetary heist, and destructive malware operations. The group was established for supporting the North Korean nuclear and ballistic-missile program by the means of cyber espionage and monetary heist. Unlike many other nation-states groups, the LAZARUS 'cyber -espionage in most cases have financial goal. The number of the group members is unknown. Cyber security experts categorize the group as Advanced Persistent Threat (APT) due to its characteristics. Different cyber security firms have given the group different names: Lazarus Group (Kaspersky), Labyrinth Chollima (CrowdStrike), Group 77 (Talos), Hastati Group (SecureWorks), Whois Hacking Team (McAfee), NewRomanic Cyber Army Team (McAfee), Zinc (Microsoft), Hidden Cobra (Trend Micro), Appleworm (?), APT-C-26 (Qihoo 360), ATK 3 (Thales), SectorA01 (ThreatRecon), ITG03 (IBM). Presumably, due to its three main missions the group has three subgroups. Each has special mission, but they exchange information, tactics and software tools.

2.1. The "LAZARUS" subgroups

Subgroup 1: Andariel aka. Silent Chollima

Andariel: The subgroup focuses on South Korean governmental organizations and businesses by using specially tailored malicious cyber operations. "Andariel" is also responsible for developing and creating unique malware to hack into online poker and gambling

sites to steal money. This subgroup carries out malicious cyber activity against purposefully selected South Korean government personnel and military officers to gather intelligence.

Subgroup 2: BeagleBoyz

BeagleBoyz: This group is responsible for the sophisticated cyber-enabled ATM cash-out campaigns identified as "FASTCash" in October 2018. Since 2016, the group has perpetrated the FASTCash scheme targeting banks' retail payment system infrastructure. The BeagleBoyz's bank robberies posture severe risk for firms beyond reputational harm and financial loss from theft and high recovery costs. The BeagleBoyz have attempted to steal nearly $2 billion since at least 2015, according to public estimates (Us-cert.cisa.gov. 2020).

Subgroup 3: Bluenoroff aka. APT 38 or aka. Stardust Chollima

Bluenoroff: A subgroup focused on attacking foreign financial institutions. They are responsible for a wide array of financial theft incidents, including the notorious SWIFT attack in 2016 when attacked dozens of banks in 11countries. After this series of attacks they managed to get away with $81million.

2.2. The activities of the "LAZARUS" groups

The group popped up in 2007, when in the course of „Operation Flame" action attacked important South Korean governmental institutions paralyzing financial and political webservices. Since this action the group has been in the focus of cyber security firms because dozens of attacks can be attached to this group. Listing these attacks would exceed the frames of this study, but some of them worth to mention because of their characteristics. The most famous, and nefarious attacks are e.g the "Blockbuster" attack against the Sony Pictures in 2014, or the attack against the international financial wire system (SWIFT) in numerous countries in 2016, where the criminals stole $81 million. The most outrageous action was the spreading of the WannaCry ransom worm that infected more than 300 thousand computers in more than 150 countries (Hern & MacAskill 2017). One of the publicly identified victims was the United Kingdom's (UK) National Health Service (NHS). More than one third of the UK's secondary care hospitals, other emergency services, and eight percent of general medical practices in the UK were crippled by the ransomware attack. As a result of the attack more than 19,000 appointments were cancelled and the recovery costs exceeded $112 million. It was the biggest known ransomware outbreak in history.

Besides the banks the ATM machines are also in the target cross of the LAZARUS group. The attacks against the ATM machines can be attached to the BeagleBoyz subgroup that withdrawn money from ATMs in more than 30 countries. According to public estimations the group tried to steal more than $2 billion since 2015. In addition to the robberies they install destructive malwares on the victims' computer. As a result of a such a kind of attack an African bank wasn't able serve its customers for two months (Us-cert.cisa.gov. 2020), (The Economic Times 2019).

With the growing popularity of the cryptocurrencies in the last few years the group turned towards the crypto-exchanges exploiting the partial anonymity of the crypto currencies. Besides the cryptocurrency stealing they also used these currencies to launder the robbed and stolen money. According to a United Nation report as of mid- 2019 North Korea approximately gained more than $2 billion by attacks on banks and crypto currencies (Bitcoin, Ethereum, Ripple and so on…) (Arquilla 2021, 4).

Owing to the sanctions and bans on the trading and the new technologies, and the resourceless economy the country has no other choice than stealing the cutting-edge technologies from the developed countries. In order to acquire the advanced technologies, they launched numerous attacks against the defense sphere, universities, research labs around the world e.g in the "Ghostsecret" action just to name one. During the course of this action the group attacked educational, telecommunication, critical infrastructures systems of more than

17 countries (including the USA) in the early of 2018. The group continuously develops its cyber capabilities. The Kaspersky lab discovered a new malware framework of the "LAZARUS" that is able to attack the IoTs with the aim of exploiting them in their further attacks. The Kaspersky lab published that the group also developed a special malware framework with a set of plugins that is able to work in any popular operating systems including MS Windows, Linux, IOS just to name a few (Lemos 2020). The group doesn't shy away from buying information on high value networks from cyber-criminal groups either. The researchers of the Kaspersky Lab during their investigation found the "LAZARUS" group among the customers of the Trickbot cybercriminal group that sells information on high value networks.

In the beginning the group focused on South Korea, and the US than they expanded their interest actually to the whole world. Today there is no country that can feel safe from the North Korean cyber-criminal group. In order to shed some light on the volume of the campaign here is a short list about the concerned countries: Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam. This short list proves that the "LAZARUS" group's activity is global in nature.

2.3. Notable tactics

In the next section some of the notable tactics of "LAZARUS" will be presented. These technics form a complex system that helps the group achieve its aims and hide their traces, and in some cases destroy the target infrastructures in addition fostering the basis of the plausible deniability.

Disruption: The disruptive technics such DDOS attacks, hard disk wipers, MFT destroyers, or wipers are used in destroyer actions when the aim is to paralyze or destroy the enemy's systems.

Misdirection: The group often disguises its actions as hackctivist activities claiming the responsibilities for these virtually fabricated groups like „GOP", „WhoAmI, or New Romanic Army". They also tried to emulate the modus operandi of hacktivists by defacing web pages and leaking information. It is not uncommon that the "LAZARUS" plants false flags inside their tools to distract the suspicions from itself. In the "KLIPOD" backdoor,e.g. they used Romanized Russian words for backdoor commands.

Protectors: The "LAZARUS" uses commercially available protectors (e.g. exepackers) for its tools. Although, in some cases they use during their attacks both protected and unprotected versions of their tools on the same target.

Anti-Forensics technics: They separate their malwares into function based components. It is mainly the feature of the "Bluenoroff" sub group. The group also tries to curb the reverse engineering by obfuscating the codes.

Command line tools: They prefer to use the command line backdoors, and installers and the use of special arguments for execution. These arguments can be among others e.g. the IP address of the C2 server, or passwords. The installer of the "Nestegg" framework, or the "KLIPOD" backdoor are good examples for such tools.

Disk wipers: These tools can be used as destroyers, but in the recent years they are used to destroy the traces of the groups' activities. They use special tools to wipe the traces without destroy the system. The group prefers to use MFT table wipers, prefetch wipers, registry, and event log wipers just to name a few.

2.4. Technical and operational support from abroad

North Korea receives valuable support from China, and India. These countries provide it with academic training, cutting edge technology, and operational support in addition they

ignore the North Korean violations of the international agreements, and also ignore the sanctions against North Korea.

China

The North Korean crime syndicates employ Chinese citizens who have access to cutting edge technologies to support their actions. In March 2020 the US Department of Justice charged two Chinese nationals who tried to launder over 100 million worth stolen cryptocurrency in favor of North Korea. The investigation found evidences that proved the link between the Chinese nationalities and the "LAZARUS" group.

North Korean students often study in China at top science and technology universities where they can access to the newest technologies. As it mentioned above thousands of guest workers are employed in the centers of the advanced technologies in China.

The Chinese government has official academic partnership (2020-2030) with the North Korean government which was renewed in 2019 (Bartlett 2020b).

India

India is well known for its high level IT expertisement and its lax stance on North Korea. India's Centre for Space Science and Technology Education in Asia and the Pacific (CSSTEAP) offers postgraduate diploma courses in science and technology for North Korean nationals. The CSSTEAP provides access to the most advanced technologies, computers and cutting-edge software solutions, and hardware for the North Korean students and scientists. This help is vital for the North Korean hacker campaigns created for fostering the funds for the its nuclear program. The reader can find North Korea among the 16 signatory countries on the homepage of the university (https://www.cssteap.org/international-linkages).

Conclusions

The „LAZARUS" group is a typical example of a state sponsored cyber-criminal group that poses threat for practically the whole world mainly for field of the financial system, cutting-edge technologies, education, and telecommunication. The end of its course of action can't be foreseen today. The North Korean government or policy can't be stopped by international bans or sanctions especially while it has strong supporter countries. It seems that the „LAZARUS" or its descendant groups will work while the North Korean ideology and policy are in power.

BIBLIOGRAPHY:

ARQUILLA, John. 2021. Bitskrieg. 1st ed. Cambridge: Medford: Polity Press.

BARTLETT, Jason. 2020. Exposing the Financial Footprints of North Korea's Hackers. [online] Cnas.org. Accessed on October 2 2021. URL: https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers

BARTLETT, Jason. 2020. „Why Is North Korea So Good at Cybercrime?". Thediplomat.com. Accessed on June 16 2021. URL: https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/

BERMUNDEZ, jr, Joseph. 2010. „A new emphasis on operations against South Korea? 38 norths special report:". 38north.org. Accessed September 16 202. https://doczz.net/doc/5259579/a-new-emphasis-on-operations-against-south-korea

Center for Strategic & International Studies. 2014. „The Organization of Cyber Operations in North Korea". Washington DC: Center for Strategic & International Studies. Accessed

September 17 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141218_Cyber_Operations_North_Korea.pdf

CHA, Victor, and JAMES Andrew Lewis. "North Korea's Cyber Capabilities". Center for Strategic and International Studies. December 18, 2014. p. 26.

HERN, Alex and EWEN MacAskill. 2017. „WannaCry ransomware attack 'linked to North Korea'". The Guardian. Accessed on 12 August 2021. URL: https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group

JUN, Jenny, LAFOY, Scott, and SHONN, Ethan. 2015. North Korea's Cyber Operations. [online] London, New York: CSIS, p.41. Accessed August 5 2021. URL: https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations

JUN, Jenny, CHA, Victor, LEWIS, James A., LAFOY, Scott and SOHN Ethan. 2015. „North Korea's cyber operations: strategy and responses". Washington, DC: Center for Strategic & International Studies.

LEE, Michael. 북한의 對南공작 활동(上)-34(in English: "North Korea's Intelligence Operations against South Korea,"). 2014. Chogabje.com, November 3, 2014, Accessed on August 5 2021. URL: http://www.chogabje.com/board/column/view.asp?C_IDX=58208&C_CC=bC.

LEMOS, Robert. 2020. "North Korea's Lazarus Group Developing Cross-Platform Malware Framework". Dark Reading. Accessed on August 14 2021. URL: https://www.darkreading.com/threat-intelligence/north-korea-s-lazarus-group-developing-cross-platform-malware-framework

ROK Ministry of Unification. "North Korea Encyclopedia: 5-year Science Technology Development Plan," North Korea Information Portal, November 17, 2015, Accessed 8 September 2021. http://nkinfo.unikorea.go.kr/nkp/term/viewNkKnwldgDicary.do?pageIndex=2&koreanChrctr=&dicaryId=8

SEOK, Lee and SANG-KI Kim. 중국(심양·단동)출장보고서 (in English: "Report on Travels from China (Shenyang and Dandong))". 2008. Seoul: Korea Development Institute, Accessed September 7 2021. URL: https://www.kdi.re.kr/data/download/attach/12241_28.pdf, p.7.

SEOK-WOO, Lee. 2011. 北 39호실의 새 외화벌이 수법… 리니지 아이템 해킹프로그램 판매 (in English: „A new way to earn foreign currency in Room 39 in North Korea... Lineage item hacking program sales"). [online, translated from Korean] Chosun. Accessed September 17 2021. URL: https://www.chosun.com/site/data/html_dir/2011/08/05/2011080500076.html

SEONGWOOK, Kim. 2009. 노무현정부, 북한 IT 인력양성 해마다 지원 (in English: „The Roh Moo-hyun government supports North Korea's IT manpower training every year"). NewDaily.co.kr. Accessed on October 1 2021. URL: http://www.newdaily.co.kr/site/data/html/2009/12/18/2009121800038.html

SEUNGHYUN, Lee. "남북경협,말들 많았지만 남은건 하나비즈뿐"(in English: "Despite Many Talks, hanabiz the Only Outcome from Economic Cooperation between North and South Korea,"). 2004. Tongil News, March 24, Accessed September 5 2021. URL: http://www.tongilnews.com/news/articleView.html?idxno=42717

SOONPYO Park, 사이버 공격 5년 동안 7만건..."대부분 북한 소행 (in English: "North Korea Responsible for Most of 70,000 Cases of Cyberattacks during the Last Five years,"). 2013. yTN, March 21, Accessed on August 5 2021. URL: http://www.ytn.co.kr/_ln/0101_201303211024217337?ems=12714

The Economic Times. 2019. Beware! North Korean hackers are watching your ATM transactions. Accessed on July 17 2021. URL: https://economictimes.indiatimes.com/industry/banking/finance/banking/beware-north-korean-hackers-are-watching-your-atm-transactions/articleshow/71323817.cms?from=mdr

United States Department of State. 2019. Democratic People's Republic of Korea Sanctions - United States Department of State. Accessed September 7 2021. URL: https://www.state.gov/democratic-peoples-republic-of-korea-sanctions/

Us-cert.cisa.gov. 2020. FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks | CISA. Accessed July 17 2021. URL: <https://us-cert.cisa.gov/ncas/alerts/aa20-239a

DOI: 10.53477/2668-6511-22-09

THE LGBTQ ISSUE AS A SUPPLEMENTARY TOOL FOR POLARIZATION IN POST-SOVIET COUNTRIES – THE CASE OF GEORGIA

George GEGUCHADZE, MA, Ph.D.,
Political Science Researcher, Caucasus International University, Tbilisi, Georgia.
E-mail: gogigeguchadze@yahoo.com

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

Abstract*: At present, when pandemic enters a new phase, the geopolitical confrontation between the adherents of unipolar and multipolar international security systems takes its new impetus. Besides the pandemic restrictions used widely as a tool of political pressure, the LGBTQ issue recently gained new importance. LGBTQ activists that announced pride in the Georgian capital have not taken to the main avenue of Tbilisi out of fears of violence. Instead, anti-LGBTQ groups' representatives used physical violence against media representatives because of their perceived pro-LGBTQ/Western stance. As it is known LGBTQ issue has become quite divisive not only in Georgia but in EU member countries. The present paper discusses developments in Georgia and the post-Soviet area as an example of a small proxy state of the former Soviet Union as an arena of struggle between the West and East on values shared by the most Western democracies.*

Keywords*: LGBTQ; politics; violence; Georgia; propaganda.*

Introduction

At present, the LGBTQ issue has been overshadowed by other issues in the political agenda of Georgia. These issues besides pandemic, include local elections, economic challenges and polarization of the society in general. Although, the events of July of this year related to LGBTQ issues played a substantial role in shaping polarized society prior to the severe challenges that took place later mentioned above. Society polarization has become so problematic today that the international society continuously stresses the importance of this issue to the government as well as all the political actors in the country. It seems to be a paradox that in Georgia, even those political actors that actually contribute to polarization in their political struggle, highlight the importance of overcoming it in their rhetoric. In these conditions it is clear that every issue which contains a divisive impulse might serve as a powerful tool to impede further development of the country.

At the same time the LGBTQ issue acquired a global geopolitical dimension and has become probably the most successful target for anti-Western sentiments in the post-Soviet area. Georgia is also facing substantial polarization of society regarding this issue. The polarization that resulted in confrontation between and within different institutions (media, church and the government) inside the country has become especially visible during July 5-6 events of this year.

So, the purpose of this article is to demonstrate why the LGBTQ issue has become such an effective supplementary tool for deepening the polarization within Georgian society. In this

regard, case study of the existing history of the LGBTQ issue in Georgia, the recent events held on July 5, 6 was used. Comprehensive analysis was made considering mentality, ethnopolitical, territorial, economic, military and historical issues that shall be taken into consideration. The trends reflecting attitudes towards the LGBTQ community in the nearest past and present have been analysed using the content analysis of the statements of the politicians, and the media publications. Also, the surveys made via The Caucasus Research Resource Centers (CRRC)[1] related data analysis tool the "Caucasus barometer"[2] were analyzed.

The article consists of brief description of developments of July 5-6 events regarding violence related to the LGBTQ issue followed by description of human rights mentality characteristic for the former Soviet space. Next issue discussed in the article concerns the problems (ethnopolitical, territorial, military and economic) that are used by destructive propaganda to deepen the social polarization in the country. Historical analysis was used to show the mentality problems inherited from the Soviet past. Also, we consider that traditional values, Western values are concepts that are used as opposing ones to aggravate polarization in the country.

Under traditional values we mean the set of values important for Georgian society that are close to the following definition: "Ideas that are considered to be of great importance in life and that are, or have been, transmitted from one generation to succeeding generations." As for the Western values, we mainly mean the declared EU values (The European Commission n.d.) which are common to the EU countries (inclusion, tolerance, justice, solidarity and non-discrimination). As to the concept of propaganda, we use the following definition: "propaganda is the interpretation, favorable for the propagandist, of a fact, a point of view, an argument, an idea or a value, including the purposefully distorted information, which shapes the society's opinion and can be used for misleading the society" (Urushadze 2019).

1. 2021 July 5th and 6th Events

During 2021 July 5th and 6th events in Georgia conservative forces managed to demonstrate their strength in the streets of Tbilisi, so they showed already existing trends in a new light. According to the Director of the Heinrich Böll Foundation Tbilisi Office Dr. Sonja Schiffers: "The country has never seen such an escalation of hatred aimed at democratic civil society. Members of civil society and particularly of the media and the LGBTIQ+ community experienced traumatic violence that will haunt them for years to come" (Schiffers 2021).

Actually, the LGBTQ issue is viewed by the part of society sharing conservative views in Georgia as the most controversial and weakest point in the whole set of the Western values. It is mostly perceived as agressive propaganda of LGBTQ rather than protection of the rights of humans with different sexual orientations. This issue causes a lot of controversy even inside the EU – its member country Hungary recently enacted legislation against LGBTQ propaganda, also, neighbouring countries Turkey and Russia are in the vanguard of anti-LGBTQ movement that is perceived or portrayed as a movement against Western values in general.

As San-Francisco University scholar, Tsygankov mentions "Because of the West's tendency to promote its values as "universal," many nations across the world tend to dismiss them as inappropriate and reflective of the West's power ambitions". At the same time, the author notes that Russia views itself as the proponent of traditional values: "In his 2013 address

[1] A.N.: The Caucasus Research Resource Centers (CRRC) are a network of research, resource and training centers established in 2003 in the capital cities of Armenia, Azerbaijan and Georgia with the goal of strengthening social science research and public policy analysis in the South Caucasus. See: https://crrc.ge/en/

[2] See: "Caucasus Barometer" – The Online Data Analysis tool (ODA) – https://www.caucasus barometer. org/en/about/

to the Federal Assembly, Putin (2013c) further positioned Russia as a "conservative" power and the worldwide defender of traditional values" (Tsygankov 2016).

It is important to note that background of the recent developments regarding LGBTQ issue, beating of tens of media representatives by the participants of counter-demonstration in Georgia and subsequent death (whether the death was caused by the injuries inflicted is still debated by the part of the government) of one cameraman created big outcry in the media. Despite the fact that LGBTQ pride has been cancelled by the organizers, the polarization in the capital reached its peak. LGBTQ issue revealed polarization between "conservatives" and "liberals" that went far beyond LGBTQ issue.

The events in July showed deeper polarization in the country that has not been so visible before. LGBTQ issue became the last drop of water in the basket but not as a priority for the Georgian population struggling with territorial conflicts. As it is known, the unresolved conflicts in Georgia resulted in tens of thousands IDP-es and refugees who fled mainly to the Russian Federation and in recent decades waves of economic immigration to the EU countries.

2. Human rights Issues in post-soviet Mentality

Lack of attention of the general public towards human rights issues in Georgia, namely LGBTQ issue in particular, can be attributed to many problems and challenges that are focused by the country. It is worth mentioning that the Russian Federation, using the soft power tools, is actively involved in prioritization of values in Georgia in order to achieve its geopolitical objectives. Therefore, it can use all the challenges faced by the Georgian state. Especially considering that there are a lot of issues that overshadow the LGBTQ issue even without artificial emphasis.

Human rights protection movement that includes LGBTQ community rights acquired substantial publicity in recent years. Since the late 80-es so-called non-traditional sexual orientation has not been anymore considered as a deviation from a norm, and the practices of forceful treatment have been left in the past. But, in fact, more efforts are needed in order to widely share this view in post-soviet societies, in our case - Georgian public.

LGBTQ issue was being focused primarily in the West whereas elsewhere (in the Newly Independent States of the former Soviet Union (FSU) for example in Georgia) human rights of refugees and/or internally displaced persons (IDP-es) due to protracted conflicts attracted more attention on the part of the society.

Some of the human rights, for example women rights have not been accepted in certain parts of the world. Historically, women played quite a substantial role in Georgian society. Despite these traditions, even in this regard the domestic violence rate is quite significant and increases. In 2013 domestic violence police protection orders numbered 229 whereas their number in 2019 reached around 10266. Please see the relevant figures from the State Statistic Department of Georgia . This growth can be probably explained by more attention and more awareness on the part of the police force, which is trained to react decisively. But the high growth of reported violence against women leaves less priority to LGBTQ community rights.

3. Ethnopolitical and Territorial Problems

In the case of Georgia, existing security challenges due to inability to solve ethnopolitical conflicts and Euro-Atlantic aspirations have to be taken into consideration as well. Failure to solve the problem of re-integration of its breakaway regions bordering with Russian Federation due to the overwhelming superiority of force on the part of the latter, subsequent borderization process at the former administrative borders of the now occupied

territories of the former autonomous Republic of Abkhazia and South Ossetia autonomous region, put Georgia in an extremely vulnerable situation from the security point of view. It resulted in deterioration of the position of Georgia related to its aspirations to the Euro-Atlantic structures. Militarily, the Russian militaries are stationed very close to the Georgian capital that creates a very vulnerable situation for the overall security of the country. As researchers note "As a result, from a military point of view, the separatist enclaves are safe from a conventional attack, while Russia, if needed, is able to split Georgia in two in several hours, by cutting the transport infrastructure (main highways and railways) linking the western and the eastern parts of the country, and to rapidly reach with ground troops the outskirts of Tbilisi" (Secrieru 2013).

Due to the transition process, the fact that the LGBTQ issue is not at the top of the agenda of the Georgian public can be attributed to the overall negative expectations within society expressed in the media and political narratives. Some of them can be formulated as follows: despite its substantial contribution to the international security operations led by NATO in Afghanistan and other parts of the world, assurances that the Russian Federation does not possess veto over NATO expansion, there was not much progress seen in this direction at least in the nearest future. At the same time, continued borderization at the former administrative border that is called the line of occupation by Georgia and state border of the South Ossetia and Republic of Abkhazia and Russian Federation that recognized their independence in 2008, makes integration of Georgia into the Euro-Atlantic structures next to impossible in the eyes of the substantial part of the public. These negative expectations are artificially enhanced by interested external actors even further. It is understandable that in these circumstances, LGBTQ issue is being overlooked especially by the general public.

4. Economic problems

Economic problems also add up to security challenges outlined above. Impoverishment of the population, the biggest drop in the cumulative output of production among all former Soviet Republics (at least 68% in 1994) according to the Report of the Vienna Institute for International Economic Studies (Iradian 2007) was experienced by Georgia in the early 1990-es, after the collapse of the Soviet Union. High GDP growth beginning from 2004 and onwards was impeded by a ban on Georgian exports by the Russian Federation, also followed by the armed confrontation with Russia over separatist regions. was exacerbated by the global economic crisis in 2008. Inability to recover growth combined with 2008 war consequences resulted in current low rates of economic growth, which was affected by the current pandemic especially in the sphere of tourism and related sectors. In this regard, it must be mentioned that Russian tourists contributed substantially to the tourism industry that had increased dependence of the industry on that country, which in turn was a negative indicator for economic independence and Euro-Atlantic integration.

As to the economic cooperation of Georgia with EU vis-à-vis the Russian Federation shows that the Russian market is still a better option for Georgian goods (mainly agricultural) considering higher quality requirements and competition in the EU and brand recognition of Georgian wine in the Russian Federation. This continues despite the economic ban introduced in 2006 shortly before the 2008 war in Georgia over South Ossetia and Abkhazia. According to the report of the Georgian branch of the Transparency International, there is "a high dependence of Georgian wine export on the Russian market, Russian tourists visiting Georgia and the import of Russian wheat". According to the report:"In 2013-2019, Georgian wine exports increased by USD 158 million (244%), of which USD 110 million came from sales in Russia" (Transparency International Georgia 2020).

It must be mentioned that unlike the young generation, the old generation "..appear to be even more sceptical than their neighbours in the post-Soviet space and are asking especially

for more public involvement in health and old age pensions [EBRD (2007), p. 48-49]. Dissatisfaction is particularly widespread among older adults, given their personal experience of the highly inclusive Soviet welfare model, characterized by top-down organised universal social security embedded in full-employment" (Baumann 2012).

Georgian agricultural products in Soviet times did not have to compete with international competitors as it is the case at present independent Georgia. As "In more industrialized countries, which were more integrated in the European markets to begin with, the transformation may have provoked less resistance. In more rural societies, whose economies were more dependent on the Soviet Union, the reforms led to a bigger shock and stronger resistance from certain societal groups" (Snegovaya 2017).

All the above-mentioned economic problems also explain why LGBTQ issue was not top priority on the public agenda.

5. Soviet past that is still remembered

The next issue we intend to discuss in more detail below is nostalgia towards the Soviet past. The Soviet past is being well-remembered and sometimes idealized for some seemingly obvious reasons like the existence of a social safety net, free healthcare and education (though out-of-the pocket payments were a commonplace) are considered as advantages by the substantial part of the population as compared to the present conditions.

Although it must be mentioned that ethnopolitical conflicts have already been notable before the collapse of the Soviet Union. As professor of the Sao Paulo University Angelo Segrillo mentions: "… the migratory movements of the USSR tended to sharpen the problem of regional imbalances in the allocation of labor. Carrère d'Encausse joined other voices in the West (e.g., Robert Conquest, Richard Pipes, Zbigniew Brzeziński) who pointed to several worrying areas of tension in the ethnic and demographic field of the USSR, even before Perestroika" (Segrillo 2020).

Focus on some of the differences in favorable light makes the past (e.g. Soviet Union) look more attractive than present, especially considering that a significant part of the population still struggles for survival being dependent on remittances from abroad. For example, subsistence farming still represents a major type of activity in the agricultural sector whereas Soviet collective farming is perceived to ensure less stratification in the sector as compared to nowadays. As Evelin Baumann (2012) writes "Since 1990, the proportion of industrial workers has been divided by four, with one active Georgian out of five being employed in industry in 1990, but only one out of twenty in 2007 [State Department for Statistics of Georgia (1999), p. 46; Ministry of Economic Development of Georgia (2009), p. 18]" (Baumann 2012).

Going back to the main topic, it must be mentioned that issues regarding nowadays LGBTQ rights have been addressed very negatively by the penal code, which was cancelled just in 1993. As the Ph.D. scholar at the University of Alberta Nikita Sleptcov writes, "The Yeltsin administration in 1993 excluded "muzhelozhestvo" (male-to-male sexual practice) from the Code of Criminal Offence" (Sleptkov 2018). So, LGBTQ people were perceived as "criminals" not long ago by Georgian society that was a part of the Soviet Union. Therefore, despite the fact that historically, acceptance of LGBTQ community representatives was prevalent in Georgia which enabled them to participate in public activities, the above-mentioned might be one of the reasons why the substantial part of the population still hardly accepts LGBTQ rights as something evident. The above-mentioned can be confirmed also by the surveys of the Caucasus Research Resource Centers (CRRC) (Caucasus Research Resource Center n.d.). For example, the survey showed that in Georgia majority of the respondents (45%)

think that hate speech is directed most often at the LGBT people;[3] 43% of respondents think that the LGBT persons most often are the target of the hate speech;[4] 54% of the respondents named LGBT people as a group they would not want to have as neighbors;[5] LGBT people is the group which is more often associated to the minority groups (13%);[6] 42% of the respondents think that LGBT community experiences hate crime most often in Georgia,[7] and the LGBT persons the most often became victims of the hate crime (29%).[8]

The same negative attitude is inherited by at least some former Eastern bloc countries. According to Dovilė Šukytė, Policy Analyst from the Eastern Europe Studies Centre, Lithuania writes, the Baltic states - Lithuania, Latvia, Estonia underwent significant changes after regaining independence. But at the same time, she underlines the following: "Nevertheless, they still remain more traditional and conservative than their allies in Western Europe. It is already a considerable achievement that the Baltic Pride parades have turned into support actions for the LGBT community, instead of protests against allowing the gathering. But Kremlin's propaganda portraying the EU as undermining family values and promoting same sex marriages still has its niche and has to be countered with increased awareness and tolerance" (Šukytė 2017).

Therefore, it is clear that this narrative is extensively used by the successor of the Soviet Union - Russian Federation in its anti-Western rhetoric in Georgia as well. This rhetoric has become more pronounced considering the increasing role of the Russian Federation at the international arena. At the same time according to Sabina Strimbovchi, it must be mentioned that "Another goal of Russia was not to let the western powers to come in the region, trying as well to impede foreign investments" (Strimbovschi 2015).

6. Armed Conflicts

According to its leadership, it managed to overcome challenges related to internal territorial conflicts and reached its geopolitical goals first close to the Southern border, Georgia and then in Ukraine. From the geopolitical point of view, the primary objective set by Russian leadership was to control its bordering countries and prevent their potential integration into NATO using ethnic divisions inside the countries. If former independent countries are not pro-Russian, small satellites, like South Ossetia and Abkhazia as well as breakaway/occupied Ukrainian regions with huge military presence keep security concerns low especially at the Southern borders especially. It is worth mentioning that Georgia provided fertile testing ground for new strategies and tactics: "In planning for conflict with Ukraine, Russia copied what worked in Georgia and adjusted what did not. Distribution of fresh Russian passports (pasportizatsiya), the supposed casus belli of defending the rights of compatriots, and accusations of malign Western intentions were repeated in both conflicts" (Giles and Monaghan 2014).

Russian Federation aggression towards Georgia in 2008 sent a clear message to the West. According to Giles and Monaghan et al: "…use of military force has to be considered a

[3] See: CRRC Poll: Which group do you think hate speech is targeted at most often in Georgia? https://www.caucasusbarometer.org/en/hs2018ge/HATGRT/

[4] See: CRRC Poll: Targets of hate speech – LGBT people/homosexuals https://www.caucasus barometer.org/en/hs2018ge/HSTLGB/

[5] See: CRRC Poll: Wish not to have as your neighbor – LGBT people/Homosexuals https://www.caucasus barometer.org/en/hs2018ge/NEIGBRLG/

[6] See: CRRC Poll: Which minority group comes to mind first? https://www.caucasus barometer.org/en/hs2018ge/MNMIND/

[7] See: CRRC Poll: Which group do you think experiences hate crime most often in Georgia? https://www.caucasus barometer.org/en/hs2018ge/HCRGRT/

[8] See: CRRC Poll: Targets of hate crime – LGBT people/homosexuals https://www.caucasus barometer.org/en/hs2018ge/HCTLGB/

useful foreign policy tool available to Russia, a concept validated by the outcome of the armed conflict in Georgia in August 2008, which, despite Western perceptions, resolved a number of key doctrinal challenges for Russia" (Giles and Monaghan 2014).

Events in Ukraine clearly demonstrated that not only a small country like Georgia populated by up to 4 mln people lacked resources to defend itself but even at least 10 times larger country, namely Ukraine was unable to maintain its territorial integrity due to increased hybrid capabilities of the Russian Federation. Moreover, an international agreement signed in Budapest by key states that guaranteed territorial integrity of Ukraine in exchange of refusal from nuclear warheads by Ukraine turned out to be ineffective.

On a global scale, the Russian Federation has been blamed for interference in the recent US elections, elections of EU parliament, also the Russian spies scandal in Austria represent only a few examples of the perceived attempts. According to Czech intelligence agency (BIS) "Russia [is] using puppet organizations and propaganda in the Czech Republic to stoke extremism and fuel anger toward the West" (Čižik 2017). Therefore, it positions itself as a strong military and soft power that is able to use disagreements on values that exist inside the European Union, in the West and even in the individual countries including the US.

As Emilio J. Iasiello (2017) writes "Based on its successes in Crimea, Russia is outpacing its main adversary, the United States, by leveraging the information space to bolster its propaganda, messaging, and disinformation capabilities in support of geopolitical objectives" (Iasiello 2017). Therefore, Russia's strategy towards Georgia can be described as follows: "Russia prefers to couch its Georgia strategy mainly in soft power terms that content-wise are based on a number of arguments. First, accentuating cultural and religious affinity with Georgia is for Moscow a political instrument that allows for emphasizing the incompatibility of "traditional" Orthodox values with the liberal emancipatory agenda of the EU that allegedly "calls for respecting sin" and "forgets about nations and patriotism." (Makarychev and Yatsyk 2014).

Therefore, it is clear that the defamation of the so-called Western liberal values, including LGBTQ issue, is an effective tool which is widely used by the Russian Federation in the area of its nearest neighbourhood.

7. Polarization in society as reflection the West-Russia tensions regarding values

Contradicting interpretations of the LGBTQ issue by anti-Western propaganda and real LGBTQ community rights protection contributes significantly to the polarization of the society. Despite the fact that LGBTQ issue is one of the integral parts of human rights in general, the destructive propaganda against "Western values" propagates LGBTQ issue as a threat to "traditional values".

In order to create wrong public opinion regarding the LGBTQ issue, the conservative forces use manipulation myths. One of them identified by the fact-checking and myth debunking platform[9] of the Media Development Foundation of Georgia[10] concerns the myth about same-sex marriage: "Myth No. 3: In order to join the European Union, Georgia must legalize same-sex marriage" (Reiter 2019). Being chosen by interest groups as a suitable target, LGBTQ contributed significantly to the polarization inside Georgian society and even between various institutions like Georgian-Orthodox church and part of the media. Therefore, "Rising frustration among Georgia's elites and the public with the slow pace of Western integration and increasingly effective Russian propaganda raise the prospect that Tbilisi might slow or suspend efforts toward greater Euro-Atlantic integration. Tensions with Russia will remain high, and we

[9] See: The Myth Detector, https://www.mythdetector.ge/en
[10] See: The Media Development Foundation, MDF (NGO), http://www.mdfgeorgia.ge/eng/home

assess that Moscow will raise the pressure on Tbilisi to abandon closer EU and NATO ties" (Gvineria 2017). Repercussions of the value tensions between the West and Russia added up to the polarization inside Georgia.

Euro-Atlantic aspiration of Georgia includes not only formal sharing of the values but its proper understanding. This is impeded by the still existing Soviet stereotypes, problems mentioned above and anti-Western propaganda on the part of the Russian Federation to portray "Western values" including rights of LGBTQ community as an insult to the Georgian national values and immediate threat to the security and identity.

This happens given the situation when Georgia has a high level of polarization for 10 years causing concern of the international community. External actors point out to the Georgian authorities the necessity to lower down the political temperature: "More broadly, tackling the polarisation in Georgian politics and media remains a priority" (EU commission 2021). For example, the Transparency International Georgia stated in the report the following: "The election campaign before the 2018 presidential elections in Georgia was taking place against the background particular tension and confrontation" (Transparency International Georgia 2018). ISFED underlines in social media monitoring report dated November 19, 2019 regarding the facebook propagandistic pages the following: "The monitoring suggests that these pages aim to incite value-based confrontation and polarization in the society, create irrational fears, influence public discourse and radicalize the society on ideological grounds" (ISFED Georgia 2019). Despite these recommendations, temperature continues to rise and LGBTQ issue does contribute substantially in this regard.

Therefore, radicalization and consolidation of the various groups and institutions around the opposite sides which are supporting or opposing the Western attitude regarding the LGBTQ issue actually happened. The issue itself has become a painful and difficult topic to address in the Georgian political scene.

It takes place in conditions when Georgia has a high level of polarization for several years causing concern of the international community. External actors still point out to the Georgian authorities the necessity to lower down the policial temperature. Polarization and aggressive discourse is underlined in OSCE interim report dated September 17, 2021: "Several ODIHR EOM interlocutors describe the political landscape as highly polarized, and the discourse as aggressive, with frequent accusations of disinformation being spread" (Organization for Security and Co-operation in Europe 2021). The same topic was addressed by the Chair of the Delegation of the European Parliament for relations with the South Caucasus, MEP Marina Kaljurand regarding the polarization in Georgia: "I would like to urge political parties to put national interests above party interests, to bring peace and stability back to the country and to continue with topics that really do affect people on daily basis (Kaljurand 2021). Despite these recommendations, the polarization temperature continues to rise and LGBTQ issue does contribute substantially in this regard.

Conclusion

Considering all the above-mentioned, the propagandistic attacks targeting the Western values can be considered as a strategy for polarization of the society, and LGBTQ issue as its implementaion tool.

It would be mentioned that LGBTQ issue gains more importance and can be considered more closely as a potential divisive point not only between Russia and the West but also between Georgia and the West. Unlike Hungary and some other countries, this issue may become an additional divisive value that may further hinder Euro-Atlantic aspirations that have already been seen by some Georgians with scepticism.

Considering the above-mentioned fact that the public consensus regarding LGBTQ issue in Georgia has not been reached, attempts to advocate LGBTQ rights causes strong opposition on the part of the conservative part of the society. In the given context, this struggle that takes place in Georgian society results in such an extent of radicalization that the state becomes vulnerable in terms of its security.

Provided the above-mentioned, the options of the government are limited and response to even cases of grave violations of human rights regarding LGBTQ community rights are being labelled as politically motivated. This in turn, impedes development of the country, raising awareness of the society and its consolidation based on human rights values. The government that attempts to get political dividends especially considering the local elections makes no effort to raise awareness on LGBTQ issue.

Since anti-Western propaganda portrayed LGBTQ community as a "fifth column" aimed at subduing "main" or "traditional" values, this community shall be supported by reminding what the basic human rights values are. Unfortunately, it will be reasonable to raise awareness regarding human rights not by pride parades but by educating on human rights in general including rights of LGBTQ community and inadmissibility of violence.

BIBLIOGRAPHY:

BAUMANN, Eveline. 2012. "Post-Soviet Georgia – It's a long, long way to "Modern" Social protection." *Economies et Societes, Serie*. URL: https://horizon.documentation.ird.fr/exl-doc/pleins_textes/divers12-07/010056159.pdf

Caucasus Research Resource Center. n.d. URL: https://crrc.ge/en/

ČIŽIK, Tomáš. 2017. "RUSSIAN INFORMATION WARFARE IN CENTRAL EUROPE." In *Information Warfare – New Security Challenge for Europe*, CENAA. URL: https://www.researchgate.net/publication/322695565_Information_Warfare_-_New_Security_Challenge_for_Europe

EU commission. 2021. "Georgia: EU report highlights the need for political compromise to continue the reform momentum." URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_425

GILES, Keir, MONAGHAN, Andrew. 2014. "Russian Military Transformation - Goal In Sight?", *Strategic Studies Institute, US Army War College.* URL: http://www.jstor.org/stable/resrep11669

GVINERIA, Shota. 2017. "Information Warfare as Russia's Hybrid Warfare Tool." In Information Warfare – New Security Challenge for Europe, edited by Tomáš Čižik, CENAA. URL: https://www.researchgate.net/publication/322695565_Information_Warfare_-_New_Security_Challenge_for_Europe

IASIELLO, J. Emilio. 2017. "Russia's Improved Information Operations: From Georgia to Crimea." *The US Army War College Press* 47 (2). URL: https://press.armywarcollege.edu/parameters/vol47/iss2/7/

IRADIAN, Garbis. 2007. *Rapid Growth in the CIS: Is It Sustainable?* Analytical, Vienna: The Vienna Institute for International Economic Studies. URL: https://wiiw.ac.at/rapid-growth-in-the-cis-is-it-sustainable-dlp-427.pdf

ISFED Georgia. 2019. *Propagandistic Facebook Pages Aim To Provoke Irrational Fears and Polarization In The Society.* Social Media Monitoring Report. URL: https://www.isfed.ge/eng/sotsialuri-mediis-monitoringi/propagandistuli-Facebook-gverdebi-miznad-isakhavssazogadoebashi-iratsionaluri-shishebisa-da-polarizatsiis-gaghvivebas-

KALJURAND, Marina. 2021. *Speech of Marina Kaljurand* Radio Liberty Georgian Branch website. URL: https://shorturl.at/dqPTZ

MAKARYCHEV, Andrey, TARTU, Alexandra, and YATSYK, Kazan. 2014. "Russian World", (Non) Soft Power: Putin's Serpentine Policy in the South Caucasus." *CAUCASUS ANALYTICAL DIGEST*. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CAD-67-68-2-6.pdf

Organization for Security and Co-operation in Europe. 2021. "Georgia, Local Elections." Interim Report. URL: https://www.osce.org/odihr/elections/georgia/498261

REITER, Anja. 2019. *Most popular myths about LGBT people in Georgia.* Media Development Foundation. Tbilisi, December 16. URL: https://www.mythdetector.ge/en/myth/most-popular-myths-about-lgbt-people-georgia

SCHIFFERS, Sonja,S. 2021. "Pride and Prejudice: Georgia after the Escalation of Violence against Civil Society." *ge.boell.org.* July 15. Accessed July 15, 2021. URL: https://ge.boell.org/en/2021/07/15/pride-and-prejudice-georgia-after-escalation-violence-against-civil-society

SECRIERU, Stanislav. 2013. "Protracted Conflicts in the Eastern Neighborhood: between averting wars and building trust." *BCT Neighbourhood Policy Paper*. URL: https://www.khas.edu.tr/cms/cies/dosyalar/files/NeighbourhoodPolicyPaper(06)(5).pdf

SEGRILLO, Angelo. 2020. *The Decline of the Soviet Union.* 1. São Paulo: University of São Paulo. URL: http://lea.vitis.uspnet.usp.br/arquivos/angelosegrillobookthedecline ofthesovietunion.pdf

SLEPTKOV, Nikita. 2018. "LGBT World Politics – Political homophobia as a state strategy in Russia." J*ournal of Global Initiatives: Policy, Pedagogy, Perspective:* 12 (1). URL: https://digitalcommons.kennesaw.edu/jgi/vol12/iss1/9

SNEGOVAYA, Maria. 2017. "Conservative Turn in Eastern Europe: Political Conservatism in Russia." *Desenvolvimento em Debate* 5 (1). URL: https://revistas.ufrj.br/index.php/dd/article/view/32163

STRIMBOVSCHI, Sabina. 2015. "Azerbaijan's Balanced Foreign policy trapped in a volatile geopolitical context." *EUROPOLITY* 10 (1): 121-134. URL: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.121-134.pdf

ŠUKYTĖ, Dovilė. 2017. "Russian information Warfare in the Baltic States and Possibilities to Resist." By Information Warfare - New Security Challenge For Europe, edited by Tomáš Čižik. Bratislava: Centre for European and North Atlantic Affairs (CENAA). URL: https://www.researchgate.net/publication/322695565_Information_Warfare_-_New_Security_Challenge_for_Europe

The European Commission. n.d. *The EU Values.* URL: https://ec.europa.eu/component-library/eu/about/eu-values/

Transparency International Georgia. 2020. *Georgia's Economic Dependence on Russia: Trends and Threats.* Tbilisi, May 04. URL: https://transparency.ge/en/blog/georgias-economic-dependence-russia-trends-and-threats

Transparency International Georgia. 2018. *Hate speech and polarization in the pre-election period.* December 06. URL: https://transparency.ge/en/blog/hate-speech-and-polarization-pre-election-period

Tsygankov, Andrei. 2016. "Crafting the State-Civilization Vladimir Putin's Turn to Distinct Values." *Problems of Post-Communism* 63 (3): 146-158. URL: https://doi.org/10.1080/10758216.2015.1113884

Urushadze, Maya. 2019. "Projecting the Foreign Propaganda on the Georgian Politics." *Ante Portas – Security Studies* 12 (1): 53-65. URL: https://doi.org/10.33674/220194

DOI: 10.53477/2668-6511-22-10

FUNCTIONS AND PRINCIPLES OF ENSURING THE SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS IN THE CONTEXT OF CYBER THREATS

Lucian SCÎRTOCEA,
Ph.D. Candidate, National Defense University "Carol I", Bucharest, Romania.
E-mail: lucian.scirtocea@yahoo.com

Abstract*: Considering the NATO and EU membership and in the context of new cyber threats, ensuring the security of information and communication systems has become a priority for both public institutions, private companies and the Romanian Army. In this article the aim is to present the main functions and principles of ensuring the security of information and communication systems in the context of the evolution of the IT @ C field.*

Keywords*: information security; cyber threats; computer and communication systems; cyber attacks; security of information and communication systems.*

Introduction

Cyber threats represent a new generation of security challenges, aimed at the defense capacity of states, as well as the personal security of citizens.

Information security threats are a problem for many individuals and also for corporations.

The Internet is the main source of IT security risks. Cyber attacks organizations have an increasing frequency: malicious websites, phishing or spam emails or unsecured cloud computing services can be sources of viral and malware infections, which can lead to the deletion or theft of key data and , by default, to financial losses.

In recent years, the complexity of cyber attacks has increased rapidly, in a single attack being incorporated both elements of social engineering and malicious software.

The sources of cyber threats are diverse: hackers, frustrated people, criminal organizations, extremist political groups, fanatical religious movements, hostile intelligence services, terrorist groups.

Cyber attack is the act of exploiting or attempting to exploit a vulnerability of a computer system without authorization.

Current cyber attacks are able to bypass conventional security mechanisms, by using techniques aimed at identifying and exploiting existing vulnerabilities, obtaining an access point in computer and communication systems, downloading computer viruses without users detecting abnormal behavior.

1. The main types of cyber security threats

Cyber threats are becoming an increasingly present impediment in our lives. Moreover, some experts are already talking about a "cyber war", the most eloquent the example being the United States, which is already dealing with the conflict cybernetic as a terrorist type (ENISA, 2012, 2).

The cyber threats in the online environment are constantly growing. Cyberspace it will always be animated by the continuous race between the attackers and those affected by them attacks.

The following are the *main cyber threats to the security of information and communications systems*.

Drive-by exploits can automatically exploit vulnerabilities in software installed on a PC without interacting with the right user. When a user visits a site that contains drive-by exploits (ENISA, 2012, 2), vulnerabilities can be exploited in browser, its plugins or the operating system to install malware on your PC without the user's knowledge.

There is also the possibility that the attackers will design a special site (fake website or even phishing) to infect those who access it. Thus, to determine users accustomed to visiting it, they resort to a strategy based on spam emails (sending of unsolicited messages by the recipient) containing links to such illegal sites.

Malware is malicious software such as spyware, ransomware, viruses and worms (The University of North Dakota, n.d.). Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software.

Code injection: This type of threat includes well-known attack techniques against applications web, such as SQL Injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. Attackers who generate such an attack try to extract data, steal credentials, take control of the targeted web server or promote malicious activities through through the exploitation of web application vulnerabilities. In recent years, the most common vector of attack against web applications is SQL Injection (ENISA, 2012,14-15). Moreover, such attacks are popular among groups hacktivist.

Denial of Service. A *Denial of Service attack* is an attempt to affect the availability of some computer or electronic communications systems/services (Orion Cassetto, 2019). The target system is attacked by the transmission of a very large number of illegitimate requests, which consume resources its hardware or software, making it unavailable to legitimate users.

Social engineering attacks act by misleading users into disclosing confidential information. Social engineering attacks include: Phishing attacks, Spear Phishing attacks as well as homograph attacks. Phishing is a form of online scam that involves the use of scams techniques for manipulating the identity of some people/organizations to obtain some material advantages or confidential information **(**William Goddard, 2021). Spear phishing attacks are a specific form of phishing in which attackers target privileged users within certain organizations. Homographic attack: represents the way in which the aggressor creates a fake website, with a web address very similar to a legitimate website and with the same look. Users are not aware that they are not on a real site buying non-existent goods and services by entering confidential data specific to the cards used.

Ransomware. A type of threat that takes the form of fake software used by cybercriminals to lure users to their malicious purposes (Linda Rosencrance, n.d.). The victim's computer is locked, typically by encryption, which keeps the victim from using the device or data that's stored on it. To regain access to the device or data, the victim has to pay the hacker a fee. This type of threat is spread by various methods such as social techniques engineering, trojans, exploitation of vulnerabilities (especially java).

Spam. Unsolicited electronic messages, most often commercial in nature, that do advertising for products and services, being used by the e-marketing industry and by to site owners with indecent content (ENISA, 2013, 26). Usually spam messages are sent by computers infected with Trojans, which do part of a botnet (a network of compromised computers used to send spam, or attacks on websites without the knowledge of computer owners respectively). Spam messages, although not a malicious program in themselves, can include attachments containing such programs, and send users to dangerous websites.

Sources of cyber threats. Common sources of cyber threats include: *state-sponsored—cyberattacks by countries, terrorists, industrial spies, organized crime groups-criminal groups, hackers, malicious insider* and *cyber espionage.*

2. Functions of securing information and communications systems

In order to reduce the threats, vulnerabilities and risks to which information and communication systems are subjected, the security of these systems requires the fulfillment of certain functions, namely:

Ensuring confidentiality, as a specific function, involves protecting a channel for transmitting information flow and information against unauthorized access and disclosure.

Confidentiality ensures the access of users only to the information specified in the security certificate. Authorized and official access to information for the institution's staff is materialized in a security certificate and in the "need to know" according to the duties of the position in the organizational chart.

Through privacy services, data and information from computer and communications networks will not be accessed and will only be available to authorized users, even if this data is stored on servers or workstations, respectively in transit through the network.

The second function, *ensuring integrity*, involves keeping information unaltered in the face of threats of any kind, as an action of human, technical or natural factors.

Integrity is ensured through the use of specific security mechanisms and products such as encryption, digital signatures and mechanisms for detecting unauthorized access.

In communications networks, integrity is approached in a specific form, called authenticity, which ensures that the data source is verified, the workstation and the user are determined, and that the time at which the operation was performed is integrated.

Integrity is ensured by:

- prevention of actions to modify data or programs by unauthorized users;
- preventing the operation of unauthorized or incorrect modifications, made by authorized operators;
- maintaining data and programs unaltered.

Ensuring availability is the function of ensuring access to and use of information and services only by authorized personnel.

Lack of availability may result in refusal of service or loss of data processing capacity, as a result of natural disasters (earthquakes, floods, etc.), accidents (fires or floods caused) or destructive human actions.

Four types of measures are important to *ensure availability*: *physical, technical, administrative and personal*.

Physical measures include access control, fire and humidity detection and warning systems, data restoration facilities outside the data processing premises.

Technical measures include fault tolerance mechanisms, access control applications to prevent disruption of services by unauthorized persons.

Administrative measures are in addition to issues related to access control policies and operating procedures, emergency response plans, user training.

Proper training of operators, programmers and security personnel is a special measure, with a focus on avoiding various availability disruptions.

As a distinct function, ***non-repudiation*** involves the removal of any uncertainty about the source or destination of a transmission, by using a reliable record that can be independently verified to establish the origin/destination of the information.

Without being a specific function, ***the audit*** represents the creation and protection of some necessary evidence in the process of investigating some facts generating security events.

The tests can be concretized in activity logs that record a series of data such as: usernames, time moments and associated actions.

Very important in ensuring the functioning of information and communication systems, ***restoration*** is the function by which information and systems can be restored if their availability has been affected.

Restoration is perhaps the most important function if one or more functions have not been performed successfully.

The functions of ensuring the security of information and communication systems become critical when we approach the fields of national security, as failure to fulfill any of them leads to compromise of information and failure to perform missions, resulting in loss of life, property damage and rescheduling or performing additional missions.

3. Principles of ensuring the security of information and communication systems

Understanding and assuming the general p*rinciples of ensuring the security of information and communication systems* will help security officials in the process of implementing security measures, to allocate the necessary resources to these specific activities, to understand the role of analysis and the tools it offers.

The first principle of ensuring security is that *there is no absolute security*. Understanding this principle will help staff with responsibilities in the field of information and communication systems security to decide what information is considered vital for different organizations as well as how to allocate the necessary funds for the implementation of security measures.

The second principle refers to ensuring the security of information and communication systems *must be carried out in depth, layered,* as a strategy to ensure information security.

Ensuring layered security is known as securing information in deep electronic format. This way of ensuring security provides us with the three elements necessary to protect information infrastructures, namely: prevention, detection and response. This in-depth security strategy provides us with answers to how to design these three elements so that if one element is weakened or outdated the other two elements can be further strengthened.

The third principle of ensuring the security of information and communication systems refers *to the fact that in the moments when they are left unattended, the staff tends to take the most uninspired decisions regarding the security of information in electronic format.*

Another principle, the fourth, refers to the fact that ensuring the security of information and communication systems depends on *two major components, namely those on the operation of information systems according to the established parameters and on ensuring the functions and requirements to be implemented and tested on these computer systems*. Functionality describes what a computer system needs to do. Assurance of functions and requirements describes how the system should be implemented and tested.

The fifth principle refers to *risk analysis.* This principle is very important to understand and analyze the value of information conveyed in information and communication systems in order to be able to design an appropriate security system following the analysis of existing threats to the information system and the amount of resources needed to do so.

The sixth principle refers to the fact that the *oversupply of measures to ensure the security of information and communication systems or the increase in the complexity of measures designed at the level of IT infrastructure*s without taking into account the value of the information we want to protect can be an enemy of security. rather, they can be a security vulnerability.

The seventh principle maintains that the *lack of decision-making, uncertainty and doubts of those responsible for ensuring security* are not the preconditions for a good way of carrying out specific activities.

The eighth principle refers to t*he way in which personnel, processes and technologies are designed and implemented to ensure the security of information and communication systems.* These measures are carried out in such a way that certain activities are carried out in compliance with the rule of the two. In order to avoid the occurrence of certain errors of judgment, activities are implemented so that certain activities are supervised by staff with responsibilities in the field of security assurance.

The last principle refers to the way in which *discussing vulnerabilities in ensuring the security of information and communication systems is a beneficial thing for ensuring security.* Hiding certain security vulnerabilities is not a solution.

In conclusion, understanding and implementing these principles listed above will help staff with responsibilities in ensuring the security of information and communication systems on how to manage information infrastructures in terms of security. How to allocate, distribute and plan the resources needed to ensure the security of information and communication systems is in fact the great challenge that security staff face.

4. The main preventive measures and technical solutions against cyber threats and attacks

In order to *prevent increasingly advanced security threats*, it is important that cybersecurity is addressed in a stratified manner. The main steps to ensure the security of information and communication systems are:

- risk assessment;
- social mentions Monitoring;
- reducing vulnerabilities.

The main measures meant to prevent and treat the effects of *counter cyber threats* are the following:

- securing the IT system;
- creating security plans;
- disaster recovery plans;
- risk assessment;
- email security;
- implement authentication solutions;
- endpoint security;
- firewall and network protection;
- reducing IT security vulnerabilities;
- web content filtering;
- data protection.

For the prevention and successful management of these threats, any organization it should consider implementing and complying with security policies cybernetics comprising:

- installation of antivirus solutions;
- implementation of appropriate data back-up policies;
- constantly updating the applications and systems used for removal possible vulnerabilities;

- restricting access from the Internet to internal systems (restriction RDP access and implementation of two-step authentication, closing unused ports for exposed IT&C systems;
- changing passwords regularly and ensuring a level of complexity their high;
- establishing an awareness policy regarding activities subsumed to social engineering (phishing, spear phishing);
- segmentation of IT&C networks;
- establishing a cyber security incident response plan in view increasing the level of resilience of IT&C systems and networks within the organization;
- training and testing employees' reaction to cyber incidents.

We will introduce you below with some *Technical solutions*[1] (Google, Romanian intelligence service, Press releases, 2021) used to prevent *cyber attacks* on IT and communication infrastructures as follows:

- using an updated antivirus solution;
- update operating systems and all applications used;
- frequent change of passwords of all users, respecting the recommendations of complexity;
- periodic verification of all registered users, to identify new users, added illegally;
- backing up critical data on offline data carriers;
- keep encrypted data in the event that an decryption application may appear in the online environment.

Conclusions

Cybercriminals end up using more and more advanced methods for implement attack vectors that are undetectable and difficult to neutralize.

It is becoming increasingly clear that mobile technology is and will become more and more exploited by cybercriminals. Threats already known and run in the traditional IT space will also prevail on mobile terminals. Proliferation of devices mobile will lead to an increase in socially generated abuse mediate.

The criminal activity that takes place in the online environment is new to us at the moment perspectives: malware consumption, cyberhacking tools and services, the emergence of digital currency and anonymous payment services.

Organizations, public or private, that hold and manage personal data or who provide essential services to the population, will be the most targeted by the attackers cybernetics in search of financial gain.

In the future we will deal with the theft of credentials, including bank details, both of customers as well as employees, by sending phishing or spear emails phishing, or by compromising POS (point-of-sale).

Phishing/spear phishing will continue to be the preferred methods of distribution of malware, given the high success rate of this mechanism, generated in largely due to the non-application of security policies as well as the security culture, including cybernetics, insufficient users.

The field of ensuring information security in electronic format in the conditions of new cyber threats becomes a particularly important and complex activity to ensure the successful accomplishment of the missions entrusted and assumed by the Romanian Army, as a member of the NATO alliance.

[1] See: https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos

BIBLIOGRAPHY:

CASSETTO, Orion. June 25, 2019. "21 Top Cybersecurity Threats and How Threat Intelligence Can Help". URL: https://www.exabeam.com/information-security/cyber-security-threat

ENISA, 2012, Threat Landscape.

ENISA, 2013,Threat Landscape.

ENISA, 2021, Methodology for sectoral Cybersecurity Assessments.

GODDARD, William. May 18, 2021. "Top 25 Cyber Security Threats", URL: https://itchronicles.com/information-security/top-25-cyber-security-threats

Romanian Intelligence Service. 2021. Press releases, "Cyber attack with PHOBOS ransomware application". URL: https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos

ROSENCRANCE, Linda. n.d. "Top 10 types of information security threats for IT teams ", URL: https://searchsecurity.techtarget.com/feature/Top-10-types-of-information-security-threats-for-IT-teams

The University of North Dakota, n.d.. "7 Types of Cyber Security Threats". URL: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats

DOI: 10.53477/2668-6511-22-11

ELECTRONIC SIGNATURE, TOOL FOR OPTIMIZING THE MANAGEMENT OF INFORMATION IN ELECTRONIC FORMAT

Lucian SCÎRTOCEA,
Ph.D. Candidate, National Defense University „Carol I", Bucharest, Romania.
E-mail: lucian.scirtocea@yahoo.com

***Abstract*:** *The development of the IT & C field produces changes in the way of organizing and functioning of all civilian organizations as well as for those in the military field. The way of managing information in electronic format is a concern of specialists in both military and civilian fields in terms of optimizing the process of managing information in electronic format due to the large volume of files and documents currently operated.*

Keywords: *information security; computer and communications system; electronic signature; information management; information in electronic format; informational management.*

Introduction

The electronic signature is a mathematical application used to guarantee the authenticity of an electronic message or document.

In national legislation, the notion of electronic signature is used for an electronic data package that is logically connected with another electronic data package and also as a tool to authenticate and identify a document or message in logical association with the person who signed it (Low no 455/2001 – electronic signature, art. no. 4).

In 1999 the European Directive no. 1999/93 defines the electronic signature in as an authentication *method*" (Directive 1999/93/EC, art. no. 2 (1), 6).

Through The *eIDAS Regulation* (Regulation (EU) No 910/2014), stated in the EU Member States, regarding availability of agreed electronic security means, the *electronic signature* is mutually recognized between them, electronically signed documents having the same trust and validity as those printed on paper and signed manually (handwritten) thru writing instruments. Therefore, the concept of the electronic signature stays similar to that provided in the *Electronic Signature Directive* (Directive 1999/93/EC).

In 2014, the Regulation adopted at the EU level introduces the new concept of *"Qualified electronic signature*", which would represent a, high-*performance electronic signature created by an electronic signature generator authorized by a certificate specific to an electronic signature*" (Regulation (EU) No 910/2014, art. 3, 84).

The advanced electronic signature must be qualified in the following *criteria* (Regulation (EU) No 910/2014, art. no. 36, 104):

- to be linked to the signatory;
- to be able to identify the signatory;
- the user of the electronic signature (the signatory) has to have at hand the necessary tools to create the electronic signature with a high level of trust, under his sole control;
- any subsequent modification of the electronic signature data is detectable.

Having regard to the specialized legislation, the European Union Regulation states that a qualified electronic signature has the legal effect equivalent to a *handwritten signed signature*

(Regulation (EU) No 910/2014, art. no. 25, 100) and that a qualified electronic signature based on a qualified certificate issued in one of the State Member will be recognized in all other States Member.

According to the same regulation, advanced electronic signatures are qualified as ,,*trust services*"[1].

The legal framework of these electronic signatures is not stipulated by the eIDAS Regulation adopted at the European Union level but will be included in the national legislation.

1. Conceptual delimitations

Digital electronic signatures use internationally authorized cryptographic algorithms and are widely used in online operations (organizational management, banking, online payment services, etc.) as well as in other situations to protect the authenticity and integrity of data.

Another term used in this specific field is that of the digital signature which is often used as a larger field of application of electronic signatures and which refers to any electronic data bearing the intention to sign. It should be noted here that not all electronic signatures are digital signatures.

There are specific legislative packages on electronic signatures adopted at the level of several economically developed countries through which electronic signatures have legal significance and where it is demonstrated that the computerization of a state is closely correlated with economic and social growth by ensuring data security in that state.

Electronic (digital) signatures were used as the electronic equivalent of holographic signatures and introduced into public key encryption systems by Diffie and Hellman in 1976 (Diffie, Hellman, 1976), in the absence of a cryptographic scheme for this purpose.

Digital signatures are based on *asymmetric cryptography* (IBM, documentation cryptography, n.d.). The digital signature combines data authentication with the authentication entity. They provide an additional confidence in ensuring the security of messages transmitted through an insecure communication channel. Properly implemented, a digital signature gives the certainty that the message has been sent by the legal, original sender.

Digital signatures are legally equivalent to handwritten signatures, stamps and seals with the mention that a handwritten signature can be reproduced on a certain document by certain interested persons while electronic (digital) signatures, which are based on a cryptographic algorithm and bind an electronic identity to an electronic document cannot be copied on another document. Verifying with certainty the authenticity of the digital signature is very easy and no specialized staff is needed to do this.

The use of the electronic signature ensures the following functions regarding the security of information transmitted through IT & C, as follows:

– *authentication*; digital signatures can be used to guarantee the authenticity of the messages sender. When the ownership of the secret key of the digital signature is assigned to a certain user, a digital signature shows that the message was sent by that sender and not another;

– *integrity*; It is necessary for the sender and the recipient to trust that the messages sent / received have not been changed. If a message is digitally signed, any change to the message cancels its signature;

[1] Trust Services' are a concept defined in Regulation 910/2014 to include electronic services, consisting of the creation, verification, validation and preservation of e-Signatures, e-Seals or time stamps, e- registered delivery services and certificates for website authentication. This concept goes beyond that of 'certification services' under the E-signature Directive (Directive 1999/93/EC) as it encompasses delegated and cloud-based signature services. A Trust Service Provider (TSP) will now be able to manage an electronic signature remotely on the signatory's behalf, if its procedures ensure that the signatory remains in sole control.

– *non-repudiation* ensures that a person or organization, regardless of the activity profile, cannot deny the issue of a document/information once signed.

2. Requirements and characteristics of electronic signatures

Requirements:

– it must be easy to implement only by the person signing the message;
– it must be easy to check by correspondents;
– it must have an appropriate validity; the signature cannot be forged until it is no longer necessary for the purpose for which it was created.

Features:

– does not represent a scanned signature, an icon or a picture.
– ensures the authentication of digital messages;
– eliminates the work with papers and their related costs;
– optimizes the necessary resources in managing documents in printed format;
– protection of communications within both military and civilian organizations.

3. Classification of digital electronic signatures

There are two distinct categories of digital signatures:

– *digital signatures with message retrieval;*
– *digital signatures with annex.*

By using digital signatures from the first category, the message can be retrieved directly from the digital signature. The simplest example of construction is by reversing the role of the public and private key in the case of the RSA scheme.

Digital signing of documents is done either by using *asymmetric cryptography*, but there are also constructions that use only *hash cryptographic functions* (ENISA, 2013).

Attached digital electronic signatures are those from which the message cannot be retrieved but is additionally sent as an attachment to the digital signature. These can be easily built by applying a hash function to the message and encrypting the obtained hash.

Due to the efficiency in signing large messages, these signatures are the most used in practice. At the same time, any digital signature with message retrieval can be easily converted into an attachment signature.

A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash) (Google 2021, hash function, March 26, 2018).

The *160 - bit SHA-1* function, which resembles the MD5 algorithm, was designed by the National Security Agency (NSA) to be part of the DSA[2] (Digital Signature Algorithm). Along the way, however, cryptographic weaknesses of SHA-1 were discovered, and the standard was not approved for most cryptographic uses after 2010.

The hash functions are used as a file identifier, to check passwords, files or messages integrity, to perform certain specific protocols, and so on.

[2] DSA (Digital Signature Algorithm) – The digital signature algorithm is a standard of the United States government for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use under the Digital Signature Standard (DSS), specified in FIPS 186 and adopted in 1993. A minor revision was issued in 1996 under the name FIPS 186 -1 [1]. The standard was extended in 2000 as FIPS 186-2 [2] and in 2009 as FIPS 186-3 [3].

One of the main applications of a common hash function is to allow searching fast data in the *scatter tables*[3].

Digital signatures can also be classified according to the signing algorithm used (one-time algorithms or multiple-time algorithms).

Another classification of electronic signatures is based on the level of trust as follows: low level used for low risk documents, advanced level used for medium risk documents, and qualified electronic signature which is an advanced electronic signature based on a qualified digital certificate and provides the highest level of trust in accordance with the European Regulation eIDAS 910/2014 (Regulation EU 910/2014), recognized in all States Members and created by a professional, competent and qualified provider of reliable IT security services.

4. Digital certificate

The digital electronic signature is provided by a *digital certificate*.

In cryptography, a digital certificate, also known as a *public key certificate*, is an electronic document used to prove ownership of a public key.

According to the *legislation* (Decision no. 1259, 2001) in force, a Qualified Digital Certificate is nominal and identifies a natural person acting either in his own name or as a representative of a third party, legal person.

Qualified digital certificate (Law no. 455/2001, art. no. 18, 7): represents the proof that the certificate has been issued as a qualified certificate including the identification data of the certification service provider, the name of the signatory, the personal identification code of the signatory, the verification data of the electronic signature, the validity period of the qualified certificate, the identification code of the certificate, the electronic signature of the certification service provider, any other information established by the regulatory and supervisory authority specialized in the field.

Similar to the concept of identity card, where the obligation to issue such documents belongs to a single authority at national level, based on documents submitted by the applicant, a digital certificate is issued by certain organizations called *certification authorities*. Such an authority, in order to be accredited, must meet strict requirements and criteria in accordance with national law, so that a digital certificate issued by that authority represents a high degree of trust.

Digital certificates are generally *used for*:

– authentication and encryption of information between servers and web browsers;

– authentication and encryption of connections in a local network - LAN;

– authentication and encryption of messages sent by email within a local network or between third parties;

– authentication and encryption of connections between servers.

Digital certificates can be of several *types*:

– *certificates for internal use* – are used in local networks belonging to military or civilian organizations and cannot be used in relations with third parties because they are not issued by accredited certification authorities;

– *certificates with domain authentication* – when issuing such a certificate, the certification authority verifies only the fact that the person who submitted the issuance request owns the respective domain;

[3] *A scatter table or hash table* is a data structure that implements the interface of an associative array, namely: it allows storing pairs (key, value) and performing three operations: adding a new pair, searching and deleting the pair after the known key.

– *fully authenticated certificates* – are granted by a certification authority only after thorough checks on the organization and the domain holder;

– *certificates for signing software applications* – are used by software companies to digitally sign software codes to prevent their compromise with malware applications when downloaded from the Internet;

– *certificates with extended validation* – represent digital certificates with the highest possible level of trust.

In the mail-specific encryption (use of email services) the holder of a certificate is usually a person or organization. However, in *Transport Layer Security/TLS*[4], although the subject of the certificate is usually a computer or other electronic device, TLS certificates can identify organizations or individuals in addition to their primary role in identifying electronic devices.

5. The role of electronic signature in optimizing information management in electronic format

The information management in electronic format within organizations, including those with military specifics, is the future way of managing them. The process of migrating information from paper to electronic format is the key to optimizing the activities carried out within organizations. An important role in the implementation of these IT&C infrastructures necessary for the information management in electronic format has the electronic signature through its following characteristics:

– the electronic signature ensures advanced security in the process of authentication of documents managed in electronic format;

– the electronic signature and certificates that are issued for the authentication of electronically managed documents are recognized at European and national level;

– the electronic signature service can be used in any Microsoft Office application;

– civilian organizations and military structures choose to use the electronic signature for security and efficiency reasons, its implementation brought savings in their budgets;

– reduction of costs related to the printing of documents, the equipment necessary for the process of printing them as well as those related to the physical management of these documents (transport, logistics, security of these documents, etc.);

– ensuring the confidentiality of electronically managed data; the electronic signature guarantees the confidentiality of the transmitted data. Digital documents cannot be opened by unauthorized persons;

– the role of electronic signatures is to increase the security and trust of the activities carried out in an organization with a certain specificity, demonstrating that the messages transmitted through electronic files are unchanged;

– electronically signed documents with a qualified electronic signature are impossible to falsify. When a document is certified with an electronic signature, it is known with certainty who the signatory is;

– the electronic signature can be used for issuing the various documents necessary for carrying out specific activities in Romania as well as in the EU;

[4] A.N.: Transport Layer Security (TLS) and Secure Sockets Layer (SSL), its predecessor, are cryptographic protocols that allow secure communications over the Internet. The term "SSL" used here refers to both protocols, except in cases explicitly specified in the context. Using SSL technology provides a greater degree of privacy and security than an encrypted web connection. This reduces the risk of information being intercepted.

– in the event of litigation, the validity of electronically protected documents is easy to prove. According to the legislation governing the field of digital signatures, the legality of these documents cannot be challenged;

– employment contracts concluded at the level of both civilian and military organizations can be signed with the help of electronic signatures, thus increasing the speed of approval and entry into force of these categories of documents provided for in labor legislation;

– unlike documents managed in printed format, electronically signed documents can be printed, but the printed paper has no legal value. Thus, electronically signed documents are also managed in electronic form.

6. Limitations on the use of electronic signature

From the aspects presented above, the use of electronic signature has many advantages, but its implementation within organizations has a number of disadvantages (limitations and costs), as follows:

– the occurrence of initial costs regarding the provision of equipment used in the process of implementing electronic signatures (means of authentication such as tokens, PCs, computer networks);

– the existence of specialized staff involved in the management of these categories of equipment used in the authentication process as well as the implementation of this system, which involves additional staff remuneration costs;

– in the absence of such specialized personnel, capable of implementing and managing such infrastructure, these services must be outsourced to private companies with this specific, which involves additional costs for the operation of organizations as well as military-specific structures;

– possible security vulnerabilities in the security policy of the military structures within the Romanian Army in the situation when this specific infrastructure is outsourced to companies that have not been carefully selected and/or verified.

Conclusions

The electronic signature is a useful tool for any person or organization, including the military, in order to streamline and optimize the activities carried out, related to the way of managing files in electronic format because the electronic signature provides legal tools for authenticating documents and guarantees the confidentiality of protected data.

I consider that the existence of some infrastructures (specialized personnel and specific technique) in the Romanian Army, for managing this field, is useful and will determine the increase of the decision making speed for fulfilling the specific missions.

The training of personnel with responsibilities in this field is essential in the new global context in which information is transmitted in electronic format within the specific networks used at the level of military structures in conditions of security and with maximum operability.

The way of transmitting information in printed format with handwritten signatures and stamps, transported by mail or couriers between military units of different echelons has run its course and these activities will have to be replaced by information and communication infrastructures, ensured from a security point of view, which will manage documents in electronic format, authenticated through the cryptographic infrastructure specific to electronic signatures.

BIBLIOGRAPHY:

Decision no. 1259 of December 13. 2001. Regarding the approval of the Technical and Methodological Norms for the application of Law no. 455/2001 regarding the electronic signature.

European Parliament. 1999. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

ENISA. September 20th, 2013. Recommended cryptographic measures, Securing personal data,

Google. 2021. Hash function, March 26, 2018, URL: https://www.techopedia.com/definition/19744/hash-function, accessed in November 2021.

IBM, n.d, documentation cryptography, https://www.ibm.com/docs/ro/i/7.1?topic=concepts-cryptography

Law no. 135/2007 on archiving documents in electronic form.

Law no. 455/2001 regarding the electronic signature of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

European Parliament and the Council. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council.

WHITFIELD, Diffie; HELLMAN, Martin E. 1976. "New Directions in Cryptography", IEEE, Transactions on information theory, Vol. IT-22, No. URL: https://ee.stanford.edu/~hellman/publications/24.pdf

DOI: 10.53477/2668-6511-22-12

FROM FAKE NEWS TO REAL NEWS WITH A TWIST: DISINFORMATION AND COVID-19 NARRATIVES

Iulia ANGHEL, Ph.D.,
Lecturer, Faculty of Communication Sciences, Ecological University of Bucharest, Romania.
E-mail: iuliaanghel2@gmail.com

Abstract*: Given the major shift in perception, communication and identity triggered by the pandemic over the last two years, the use of digital tools to guide patterns of association, mobilization and action seems more powerful than ever. Although Fake News has been making headlines since the early days of globalization, its later developments revealed interesting conjectures on topics such as the rise of non-state hegemons, ascent of digital diasporas, deterritorialization, or post-politics. In this context, the distances between fake news and reality tend to be blurred by the intervention of interpretive bias, while the role of public's beliefs, latent iconography and power mythology becomes more critical. Following this argument, the paper looks at some of the emerging trends in fake news and master narratives in digital media, also tackling the implications triggered by their potential use in the context of hybrid confrontations.*

Keywords*: fake news; disinformation; COVID-19 narratives; infodemic; hybrid threats; edifices of shared meaning.*

Introduction

Even if false information that imitates trustworthy sources is not new at all, fake news phenomena became lately more pervasive both in traditional and digital strategic channels (Parker et. al. 2020, 141-142). Unquestionably, nowadays evolution and maturation of the fake news debate remains connected with trends such as post-truth dimensions of populist speech (Althuis and Haiden 2018, 4-5), decreasing trust in traditional media or shifts occurring in the information landscape. However, these major reconfigurations of the public sphere were doubled by more specific and less visible transformations. Emergence of filter-bubbles, wherein isolated publics built their own agenda, revelation of the rhetoric conditions of the individuals, able from now on the create and distribute content or the power of spinning, generating false majorities and opinion flows, all opened the road for an increasing impact of hybrid confrontations. Involving practices such as subverting sovereignty, promoting non-democratic speech or simple spread of fake news, these unconventional threats recall a hybrid strategy of collective defense (Valášek, 2018, 28-30). Aiming to address these new challenges, redrawing the informational, political, and cultural landscape, the article employs a two-step methodology. The first part concerns a conceptual reconstruction of the notion of fake news, redefining fake news as narrative constructs able to trigger biased interpretations, mostly based on cultural stereotypes. The second part engages the case study method to provide a multi-layered analysis of the recent COVID-19 disinformation, connected to widespread anti-vaccine, anti-EU, and anti-globalist narratives.

1. Fake news. From false information to edifices of shared knowledge

Contemporary attempts in developing a conceptual framework of fake news are still influenced by two key landmarks: the intention to deceive and the objective to harm or control. Academics and practitioners agreed to classify fake news into four categories: disinformation, misinformation, mal-information, and non-information (Parker et. al. 2020, 141-142). The term disinformation is traditionally defined as "constructed false message" transmitted to the opponent's communication system, to deceive and influence the target public (Bittman 1984, 49). By picturing many of the "disinformation games" as actions designed to manipulate the decision-making elite, Ladislav Bittman's influential book, *The KGB and Soviet Disinformation: An Insider's View*, highlights the role of public's segmentation in achieving long term results through the instrumentality of false information (*Idem*). Following his perspective, public opinion is "just one of the potential targets" of false information, the dissemination of the initial stimulus in a more restricted environment assuring that further transmission will be accompanied by a veracity hypothesis. When decision-makers employ a certain point of view or promote a specific approach towards a dilemmatic social or political context, they also use other genuine argumentative elements. Thus they may transform the initial false message into complex content, perceived as authentic, if reiterates many of the public's shared opinions and beliefs. Going one step further, Bittman argues that any "disinformation message must at least partially correspond to reality or generally accepted views" (*Idem*).

Yet, not every anti-establishment or critical public opinion should be considered as part of well-orchestrated propaganda campaign, since sentiments such as fear or rage may determine spontaneous concerns, affecting publics whose political preferences are far from radical or populist (*Idem*, 144). In this context, misinformation should be perceived as a non-intended mistake, conveyed as credible, but later corrected (Greifeneder et. al. 2021, 28). Misinformation is first defined by absence of intention in distorting the content and secondly by integration within target public's beliefs. Yet, authors as Martin C. Libicki consider that within new cyberspace information warfare, the credibility of the information in general can be ruined by "adding false information to it to the point where the victim must choose between misinformation (believing what is not true) or disinformation (being unable to believe what is true)" (Libicki 2007, 57). Due to its dynamic nature, information can be thus altered in multiple ways, the distances amid classic formula of disinformation (constructed false message) and misinformation (unintended distorted content) being reduced by intervention of publics.

There are many situations in which individuals or groups tend to respond to emotional stimuli and generate misinformation. Cataclysms, pandemics, social conflicts are just some of the contexts when internet users share stories and testimonies that alter the initial picture by adding plausible or intuitive elements, that were missing from their direct experience. Whether it is about atrocities committed by adverse forces or presumed threats exerted by unknown enemies, this supplementary content is added as an affiliation gesture. False memories and false witness-accounts may indicate that "participants are reporting and/or selecting false information" under pressure exerted by post-event suggestions (Ridley et. al. 2013, 31). Thence, the disinformation strategies may lead to further distortion that could engage neutral publics, influenced by the cultural context they live in.

Furthermore, these trends are potentiated by information overload. Mal-information and non-information came into prominence as secondary effects enabled by digitalization and globalization of information. Scholars as C. Wardle and H. Derakhshan affirm that mal-information "is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere" (Wardle and Derakhshan 2017, 2). In case of mal-information the focus is not in faking the content, but in emphasizing sensitive aspects, to

determine partisanship and polarization within the reception of the message (Saez-Trumper 2019: 4). At the same time, a specific content can be classified as non-information if represents "irrelevant information that obfuscates, hides or covers real or true information sought by audiences" (Yiquan and Wenzel 2014, 634). Proliferation of unclear information, creating confusion, and recursion of conspiracy theories was directly influenced by spread of COVID-19. In this context, the infodemic label, signalize the presence of too much information including false or misleading content in digital and physical environments, during a disease outbreak (World Health Organization 2020).

However, the expansion of the fake news debate beyond the classical disinformation-misinformation interplay it is motivated also by other complementary evolutions. During the global pandemic, populist discourse shaped the perception of reality, employing dominantly the phantasmatic dimension of political speech and the narrative divide between the elites and "the real people" (Cervi et al. 2021, 291-294). The claim of separating society into antagonistic groups, based on "people vs. the establishment" equation, also triggered cultural and strategic consequences (Funke et. al. 2021, 1-5). Fake news term became politicized and used in correlation with adjectives as "corrupt", "disgraceful" or "Enemy of the People" (*Idem*, 1-5), gradually creating a parallel reference. Moreover, the populists coined fake news as an interpretation and loyalty game, magnified with the support of social media.

Employing old tactics as the tendency to oversimplify the public agenda, polarizing and provocative discourses, appeals to nativist worldviews, prolongation and recovery of conspiracy theories or illusion of direct and unmediated communication with the leader, the populist actors (*Idem,* 1-12) exploited the social media logic, which tends to bring forward simple messages and emotional communication. The intersection of new media logic, populism and fake news generated what was called an "elective affinity" (Gerbaudo 2018, 746-747). Under these circumstances, the mal-information and non-information entered the fake news arena, especially as populist revision of false news significance employed the revival of cultural stereotypes, mythologies, and basic groups narratives. Even if academic literature generally defines the fake news as "false news intended to mislead audiences" (Parker et. al. 2020, 143), it is considered that the 2016 USA presidential elections served as a landmark in shifting the usage and term. Fake news became a tool used to dismiss information and facts that contradicted the mindset of a particular group, often having the function of closing the debate. One interesting consequence derived from this semantic renegotiation refers to the fact that the public's inherent beliefs and attitudes can shape the reception of fragmentary or partisan information, creating the meaning in a way which almost excludes outside control. No matter if it is about rejecting globalism, denunciating elites or distribution of social culpability, the populist mindset invites to uniformity and a decoupage technique in relating to the informational space. Jair Bolsanaro or Donald Trump strategies in molding the narrative around pandemic remain relevant case studies for this framing approach (Cervi et al. 2021, 296).

Quite often fake news could employ content that is received as novel, sensational, compelling, and activating a natural emotional response. This feature argued for the analysis of the phenomenon within an ecosystem of related terms as: 'truthiness' and 'post-fact' or deep fakes (Parker et. al. 2020, 146). First concept, truthiness implies the circumstances and context in which the credibility of a fact, an information or event seems to be acceptable for the general opinion (Berthon and Pitt 2018, 2020). More important, truthiness covers a perceptual predisposition, reduced to the catchphrase "the world is as you wish it" (*Idem*, 220). A strong example for this approach is offered by global patterns of anti-vaxxer lobbies, that engage tactics based on rejection of the basic information upon the subject and use of emotional opinions. Blending simultaneously archaic nostalgia with fear, social rejection syndrome, national mythification and millennialism, the anti-vaxxer movement offers the picture of a

distorted truthiness. A closely related element the term of post-fact may be defined as "taking a position that ignores facts" (*Idem*, 221). Known also as alternative facts strategy, the term was epitomized during a press release in 2017, when Trump's advisor Kellyanne Conway used the phrase as an exit strategy for avoiding relating the basic facts. In the end, another interconnected element of the discussion is the term of deep fake.

As a generally definition, deep fake implies the creation of false audio and video content, which presents sensational, offensive, or dramatic facts (Citron and Chesney 2018). The main role of deep fakes is to spin the trends, generating an emotional response based on rage, fear, and shock. Deep fakes tend to determine major reputational consequences, even if later fact checking exposes their falsehood. A good example for the use of this technique is the disclosure of a fake video, picturing Barack Obama using offensive language against Donald Trump (Parker et. al. 2020, 147). Intrinsically, the target audiences resonated to what they wanted, and what they were used to believe, even if the authenticity of the content was by far questionable. Yet, despite all that, the damage caused by release of such deep fake lingered in the background, due to intervention of undersurface mechanisms such as: cyclical memory, recovering fragmentary recollection of the facts, ingravescence of social divides, confirmed by emotionally appealing digital content and not lastly, the illusion of authenticity and direct participation in the circle of events.

All the elements mentioned above depend in a critical manner on the "connections between one's worldview and one's perception of the truth" (Althuis and Haiden 2018, 9-11). Scholars as George Lakoff and Mark Johnson argue that the way an individual or a group judge a statement to be true of false is decided by their understanding of the context. There is a strong connection between metaphoric systems and the claim of coherence (Lakoff and Johnson 1980, 23). Following Benedict Anderson's approach to national identity, seen as imaginative shelter of a dynamic narrative (Anderson 2006, 16), the shared knowledge needs to assure the prolongation of a structure. In this context, the basic narratives that incorporate the opinions, value-systems, way of thinking, identity, ideology engagement and main viewpoints of an individual, represent the edifices of "shared meaning" (Althuis and Haiden 2018, 9-11). Generally, edifices of shared meaning are constructed through language and grounded on imageries and metaphor. They are constantly circulated through the instrumentality of media channels, but also contain a latent dimension. S. Huntington's seminal work in political anthropology revealed the presence of a silent cultural pact in American society, proved by the emotional use of the national flag during times of uncertainty and crisis (Huntington and Dunn 2004, 3). The central hypothesis employing the edifices of shared meaning stipulates that the reception of sensational headlines, breaking news announcements or traditional fake news is influenced by their interactions with the basic shared narratives of the individual. This inherent conceptual framework operates dichotomic cuts within the mainstream information flow, favoring instead biased and partisan information. Contemporary audiences are decoding the political speech or the apparently benign false news through a rhetorically constructed conceptual framework (Althuis and Haiden 2018, 9-11). Effects of this closed interpretative circle, expelling the other side's perspective or translation of facts are further potentiated by a set of structural evolutions.

Tendencies such as the decline of scriptural information and ascent of an image-oriented culture influence the reception and perception of news, real or fake. The tribalization of image implies a decline of the group memory since the image represents an inherently metaphoric construct. The image itself has no unique meaning and can be reinterpreted in a perpetual semiotic circle. The case of false witness accounts promoting images of violence and abuse offer a critical sample of this boomerang effect. During the Ukrainian crisis a great part of the Russian active measures and hybrid approaches focused on superposing stereotypes of World War II upon present events (Khaldarova and Pantti 2016, 3-6). The master narrative was built

around images of old people in Donbas region, depicted as poorly dressed in the near vicinity of their destroyed houses, while in the background an emotional or patriotic soundtrack was running (*Idem*, 3-6). The edifices of shared meaning were put in motion to validate the story, even if the facts were contradicted by other media statements or individual testimonies. Within the same hybrid conflict, images picturing the outrage of the population and the rejection of the Russian intervention were circulated under the false claim of disavowing the 'fascist' abuses of the Ukrainians (*Idem*, 8). The situation in which we cannot agree on basic facts and the falsehood or authenticity of a message is arbitrarily decided by the viewer, announces an interrelated trend.

Filter bubbles can be defined as ideological frames (Pariser 2011, 12), generated by algorithm tendencies to deliver search results that fit the consumer profile, interests, and information behavior. Personalized news streams promote a segregation of agendas ending in ideological media territories. Filter bubbles imply intellectual isolation (Bozdag, 2013, 209), perceptive biases, confirmation fallacies and not least the illusion of a flattened, simplified, and tangible information space. Apparently, we may access real data around the globe, but all the search filters interposed amid the presumed reality and the user tend to reiterate the subject's view points and opinions. Filter bubbles may be equaled with a dynamic representation of the edifices of shared meaning, since the individual adhesion toward certain values, political models, or social manifestos is constantly recreated through the instrumentality of interactive information flows. Trumpism ascension and electoral winnings were explained in relation with this type of disruption of the information landscape (Baer, 2016). Personalized content was made responsible for shadowing the other perspectives, while fragmented publics distributed in insulated online communities created a mass self-communication (Baer, 2016). Genesis of rhetorical arenas enabling individuals to create, share and promote content on a scale never seen before, changed the traditional mediatization models. The new discovered symmetry between users and media players, proven by proliferation of labels as collaborative journalism, participatory reporting or citizens press, influenced in a critical manner the information selection mechanisms. The rhetorical revelation offered the anonymous users the opportunity to control the content, to start trends or even to act as game-changers in relation with media outlets.

Donald Trump's victory was possible under special circumstances, while the public was divided within filter bubbles and echo chambers, wherein the anonymity determined a decrease of civic and politic accountability. Individuals were liberated from formerly assumed political activism and could use the faceless virtual crowd as a cultural canvas for revealing formerly repressed or latent traditionalist or nativist affinities. At the same time, radicalization of micro-publics was connected to confirmation biases and also grounded in subsidiary processes such as the gamification of politics. Starting with Italy's social media populism, materialized in Matteo Salvini "likeability strategy" (Bobba 2019, 12) to America's dark experience of viral news, filter bubbles and echo chambers reconstructed the anatomy of the public opinion. In this manner non-information and mal-information gained relevance as strategic communication tools, able to circulate identity constructs and to shape the receptivity of certain audiences. Exploitation of edifices of shared meaning as complex forms of propaganda, inaugurated a new phase in fake news symptomatology, since they proved to be available to various actors, including grassroots movements, hybrid influencers, anti-establishment parties or populist moves.

In this context, hybrid challenges could be shifting from traditional players such as states, economic lobbies, security blocs or ideological moves to new malign and benign digitally constructed communities. Keeping in mind the aspects highlighted before, the following section addresses the intersections amid nowadays COVID-19 disinformation and the employment of cultural stereotypes, shared meanings, and fake news in the context of hybrid threats.

2. Hybrid tensions and COVID-19 fake news in recent Europe. Analyzing the narratives

The evolution of COVID-19 disinformation was strongly influenced by a set of interrelated trends such as information overload, polarization of opinions, societal divides and revival of nativist and millennialism affinities. Around the world, populism and anti-democratic forces tried to hijack the discourse on pandemic, while various state and institutional bodies were facing serious difficulties in building a response strategy against this complex crisis. Initially, disinformation was concentrated on the cause of the COVID-19 crisis, the primary narratives targeting China's strategic and politic culpability. At the very beginning, COVID-19 blame game was seen as an upgraded version of a cold conflict between United States and China (Horsley, 2020). The prospects of this confrontation were unclear at that time, the global diffusion of the virus determining, however, a change of the initial narratives. Once Europe experienced a gradual aggravation of the sanitary crisis, materialized in lockdown measures and various restrictions, disinformation crossed a localization and adaption process. In this context, COVID-19 narratives became "culturally tailored", reflecting the structural fractures and the important debates in each society (Serrano et al. 2020). A general survey of the narratives used in Europe during the COVID-19 pandemic emphasized the presence of five main typologies: health fears, lockdown fears, false cures, conspiracy theories and identity and political dispersion (*Idem*). Usually, the first three categories of narratives relate to the traditional model of fake news, employing the use of distorted information to achieve emotional responses on a certain topic. It may involve decontextualized photos and videos, appeal to fictive authority voices, doctors or researchers or impersonating the media or authorities, using false documents or deep fake content. The health fears proved to be a source for further interpretation and declination of narratives, much of the initial fake news originated under this label demonstrating an interesting uniformity. As an example, videos apparently presenting corpses of Chinese abandoned on the streets of Wuhan, were circulated in various European countries and induced panic responses, even after the false was exposed (Reuters, 2020). The visual disinformation associated to COVID-19 pandemic had a peculiar trajectory also due to diversification and fragmentation of communication channels.

Involvement of instant messaging apps complicated the facts even more, since it forced individual users to react and evaluate the content in insolated environments. In defiance to social media fake news, which rely heavy of snowballing and supportive false majorities, the texting disinformation was more difficult to pursue and counteract since it was exploiting the individual's social, cultural and informational bubble. Disinformation moved from social networks to text, mostly because lack of reactive options on behalf of regulators and institutions. Debunking of the fake news campaigns and deconstruction of their narratives was hindered furthermore by the exploitation of strong symbolic components. The call for unity, social change or civil disobedience was made in most of the cases under auspices of national, ethnic, or religious empowerment.

An example for this new disruptive practice is offered by the text messages and social media posts distributed in France in the early stages of COVID-19 crisis, advising citizens to act responsibly and to limit social interactions, as a presumed number of cases were already confirmed in their near vicinity (Banet, 2020). The information was launched in January 2020, when text messages and print screens of posts announcing COVID-19 cases in different French cities were circulated on social networks and instant messaging apps (*Idem*). The social media posts were apparently distributed by well-known media actors as BFMTV and they did not entail any criticism upon government or protest and mobilization action calls (*Idem*), while the text messages had no source indicated. Use of simple language, the appeal to social responsibility and apparently lack of perceptible benefits for the spread of this information

assured a spectacular permeability of the target groups. Although the information was soon declared false, the effects of the campaign remain strong. The main problem raised by this type of fake news resides in the difficulty to isolate and confirm the true beneficiaries. This sort of disinformation strategy affected the social climate in France, stimulated emotional responses, determined a decrease of credibility for the media system and created an environment favorable for further disinformation and misinformation. The primary false content could be linked to actions of multiple players. International security hegemons as Russian Federation or internal disruptive groups are constantly targeting a degradation of the social and political environment of the EU countries. The use of fabricated false content could serve in this case in stimulating social panic, mistrust regarding actions and competence of government and the need for immediate intervention. Populist or authoritarian political offers often benefit on behalf of this type of disinformation, recent evolutions hosted by countries as Poland or Hungary calling for reflection.

Decline of common social and cultural landmarks and downfall of mainstream media generated paradoxical interpretations of information. Infiltration of fake news was operated within the instrumentality of pervasive channels as texting, social media groups or even brochures. Social media infodemic perceptible on various channels as Twitter, Instagram, YouTube, Reddit just prepared the grounds for this strategic tournament (Cinelli et. al. 2020). Yet, individual responses to COVID-19 disinformation reflected a departure from traditional models of action and determined a reconfiguration of the stimulus-response theory (Barua et. al. 2020).

The fake news or tendentious content could be considered as a stimulus, while the personal evaluation of the target groups may play the function of feedback. Information it is tested, evaluated, and accepted as it passes the credibility test (*Idem*). Some approaches choose to address the disinformation patterns in relation with cultural benchmarks, rather than invoking the specific structure of the distorted content. Following this narrative logic, other classification of the COVID-19 related disinformation may be reduced to three categories: general misinformation beliefs, conspiracy beliefs and religious misinformation beliefs (*Idem*). This sort of reconfiguration of the theoretical debate proves once again the complex dynamic of the phenomenon and highlights the leading role of cultural backgrounds in organizing the public reactions. General misinformation beliefs as "Coronavirus is not heat-resistant and will be killed in a temperature of 26-27 degrees" or "the virus does not settle in the air but on the ground, so it is not transmitted through the air" entered the informational space almost unnoticed (World Health Organization, 2020). Unreliable information generates mistrust, skeptical attitudes and builds a basic cultural frame that rejects other perspectives (Fakhruddin et al. 2020), even if initially, this filter seems less obvious. Conspiracy beliefs, as news claiming that COVID-19 represents a biological weapon, are based on a collective interest upon the subject of bioterrorism, already present in the information environment. In the same manner, religious disinformation beliefs are only partially directed by religious bodies' interests in exploiting the pandemic. Nevertheless, religious groups aim to play a substantial role in influencing people's behaviors, fundamentalist actors around the globe competing to monopolize the spotlight of COVID-19 narratives, but grassroots response remain hard to predict and control. It is difficult to acquire control upon religious discourse since official messages can be shadowed by disruptive content. A good example of these disturbances is shown by the Romanian society divide with respect to the subject of COVID-19 pandemic religious implications. Despite the Romanian Orthodox Church's endorsement of vaccination, anti-vaxxer propaganda continued to successfully exploit religious semiotics and arguments in controlling the conspiracy narratives (Dascălu et. al. 2021). All anti-vaxxer protests shown in mainstream media or reflected by support groups in the digital space engage religious and

nationalist symbolism, often flattening the narrative until it is reduced to a patriotic call. In Romania's case, the circulation of basic edifices of shared meaning, such as the national narrative, creates complex costs in deconstructing and limiting the COVID-19 related disinformation. Mixing national flags with religious iconography and traditional village semiotics, anti-vaxxers move targets a recognition, affiliation, and loyalty game. Drawing on arguments of Barua and others, it may be considered that the borders among disinformation, misinformation and persuasive employment of cultural frames are blurred by the intervention of an emotional selection mechanism. Reliance on emotion promoted belief in false information, as several studies demonstrated a connection amid emotional messages and the decrease of discernment. Given the fact that "greater emotionality is associated with heightened belief in fake news and decreased discernment between real and fake news" (Martel 2020, 15), the use of edifices of shared meaning as vehicles for asserting partisan reflections of reality remains a tactic difficult to restrain. Debunking simple false news is targeting the exposure of untrustworthy sources or distorted content, while denunciation of cultural partisanship requires more subtle interventions.

Going back to the conspiracy and societal divide equations of fake news, a tendency toward "globalization of disinformation" was observed (Serrano 2020). The power of shared narratives resides in their capacity to structure and make sense of a chaotic reality. Previously, this function was assumed by traditional media outlets, made responsible for selection, organizing, and translating events into a common narrative, communicated afterwards to a national audience. However, digitalization implied a reconfiguration of the media patterns. The national publics are now replaced by thematic audiences, fragmented interest bubbles, infotainment consumers and other emerging categories that defy the idea of a common agenda. Even if these insulated audiences apparently support and validate the same narrative, the drivers for such reactions may be substantially different. For example, fake news concerning false cures and lockdown fears act initially as benign entry doors of nativist discourses. This layer of fake news targets cultural affinities such as environmentalist concerns and civic disobedience, inducing a gradual contextualization of the COVID-19 debate. Biased interpretation and reception of the COVID-19 disinformation may thus be perceived as a long-term process, exploiting the preexistent social divides and cultural cleavages. Segregation of the moderate and noninvolved publics and their gradual persuasion is obtained through simple and iterative means. In this context, identity and political polarization may be achieved by inflaming and circulating the latent fears and representation of a society.

Recent media dynamic disclosed that an array of far-right analogies is used to attract support and engage audiences in what was represented as a critical social and political action call. Proliferation of labels as sanitary dictatorship or COVID conspiracy engages peculiar translation within certain cultural contexts. Western Balkans and Easter Europe as a whole, experience a degradation of their democratic climate in connection with COVID-19 disinformation, carried simultaneously by well-known security hegemons and regional and local challengers. Presumed information campaigns developed both by Moscow and Beijing targeted two key messages: European citizens are vulnerable because they cannot trust their political systems and authoritarian rule may save the situation (Bentzen, 2020, 2). The main concern created by these trends is that a mix of disinformation and health diplomacy echoed also by various proxies in Europe and not only, may end in a wider influence in other sectors in aftermath of the crisis (*Idem*, 3). Health diplomacy could be defined as the practice by which states and international relations actors develop policies and programs dedicated to the improvement of global health. Nowadays, the use of the term concerns predominantly the Russian Federation's efforts to create a positive perception upon its international role and regional and global legitimacy, through instrumentality of medical help offered during COVID-19 crisis. When Moscow sent several military planes loaded with medical equipment to help

Italy to manage the COVID-19 crisis, the international perception was one of a soft power exercise (Valenza 2020, Leight 2021). Going one step further, the vaccine diplomacy played an important part in renegotiation of Russia's power brand, assuring a more positive image in the Balkans and Central and Eastern Europe (*Idem*). Information overload, narrative control, digital divides, and politicization of data will continue to convey the message that authoritarian nationalism is the only viable answer to nowadays sanitary, cultural, and political crises, while people are apparently pressed to choose between security and freedom (Idem, 3). By exploiting alienation and marginality of certain social clusters, the COVID-19 disinformation prepares a post-pandemic topic of narrative operations. However, Chinese "coronavirus diplomacy" and Moscow's aid strategy, by excellence a continuation of long span hybrid operations, could face serious competition. The employment of tactics such as concealing, disguising, coopting, penetrating, and manipulating, along with spreading conspiracy theories and increasing social polarization may determine the activation of influential edifices of shared knowledge. It was already proven that employment of identity narratives and cultural stereotypy may shift opinions and antagonize audiences on various topics and agendas. The pandemic context will come to an end, but the consequences of these unforeseen mobilizations of cultural manifestos may determine a privatization of hybrid conflicts.

The hybrid warfare label can be applied to a range of phenomena related to war and culture (Gunneriusson 2021). However, present evolution in the informational space may enable the empowerment of discrete players, exploiting the volatility and multivalence of shared narratives. The national identity argument was circulated by governments, security hegemons, grassroots moves and not least spontaneous domestic initiatives. Many European countries tried to control the national tale and to expel a hybrid use of shared identities. Yet France and Germany confronted with radicalization of anti-vaxxer protests, using nationalist arguments, while Eastern Europe disclosed an interesting conjecture amid nation and religion. Recovery of nativist claims and millennialism discourses it not new at all, Kremlin making a staple from its "return to tradition" arguments circulated on European grounds long before the Crimean case in 2014. What seems to change is the availability of such means to new entities and groups. The present dynamics of the informational realm could impose a new set of working hypotheses. First, digitalization made almost impossible to control the spread of information, while the associative patterns of individuals and the modelling of social networks also remain open to malign influences. Secondly, paradoxes of identity enabled by digital communities may determine a decline of social contracts and cultural pacts. Internet is hosting faceless crowds, mixing trolls, bots, and real individuals, and offering a fluid impression of legitimacy or majority. Reunited, these background effects may announce a new stage of hybrid threats, considering that shared narratives are already claimed by unexpected beneficiaries.

Conclusions

Neither fake of real, the news gained nowadays an interpretive layer, aggregated in the eye of the beholder. Keeping in mind Lakoff's metaphor upon edifices of shared knowledge, contemporary weaponization of social and news media may put under scrutiny previous models of social action in favor of a narrative and story-based rationality. Perhaps it is not enough to blend the right ingredients into the image-oriented and digitally based emerging culture, to achieve a desired result. Yet, the new visual syntax of contemporary news, along with other critical trends such as liquefaction of borders amid private and public space, decline of national identities, generational segregation or globalization-glocalization interplay modify the power balance in the information sphere. Nation states and international organizations face competition from shadow communities, spontaneous associative entities, or dormant cultural

groups. Hybrid threats are multiplying in connection with key matters such as civil disobedience, netwars, soft power and not at least monopoles upon interpreting and contextualizing truth, religion, and justice. Breaking news journalism and algorithmic populism (Maly 2020, 445) opened the road for distorted information selection, but the main beneficiaries of this historical fracture may not be the intended ones.

Previously, the hybrid label was employed predominantly in connection with Russia's activities in cyber operations and coercive diplomacy. Yet, attention-based media systems enhanced a democratization of populist techniques (Idem, 463), and made hybrid operations available to other players. Proxies, anti-establishment parties, and grassroots movements can negotiate their intervention in the hybrid conflicts, using classical disinformation tactics or innovative cultural methods, such as circulation of shared identity narratives. Intersections amid fake news, cultural backgrounds and populism have demonstrated the impact of soft power in undermining the existence of the European project itself. Russian and Chinese narratives were considered responsible for conspiracy theories proliferation and radicalization of certain audiences, but in time, the narratives may perpetuate and evolve autonomously, creating even more disinformation. This unfolding is further enabled by conjugated actions of image-based news and the digital version of the sleeper effect. Traditional delayed persuasion obtained through repetition of the key messages may determine a selective bias. The sources of the content or the context within the message delivered are obscured by the recirculation of the image, its special syntax expelling a unique interpretation. Traditional security hegemons or rising contenders exploited conspiracy or polarization narratives, transmitted through stereotypically visuals, but their final trajectory within the digital space remains unknown. In this ever changing symbolic and strategic battle, who the true spin doctors are, is yet to be seen.

BIBLIOGRAPHY:

ANDERSON, Benedict. 2006. Imagined Communities. Reflections on the Origin and Spread of Nationalism. London: Verso.

BAER, Drake. 2016. "The «Filter Bubble» Explains Why Trump Won and You Didn't See It Coming.". The Cut. Nov. 6, 2016. URL: https://www.thecut.com/2016/11/how-facebook-and-the-filter-bubble-pushed-trump-to-victory.html

BANET, Rémi. 2020. "Nouveau coronavirus: attention aux fausses captures d'écran sur les réseaux sociaux." AFP France. URL: https://factuel.afp.com/nouveau-coronavirus-attention-aux-fausses-captures-decran-sur-les-reseaux-sociaux

BARUA, Zapan; BARUA, Sajib; AKTARA Salma et al. 2020. "Effects of misinformation on COVID-19 individual responses and recommendations for resilience of disastrous consequences of misinformation". Progress in Disaster Science. Volume 8, December 2020, 100119. DOI: https://doi.org/10.1016/j.pdisas.2020.100119.

BENTZEN, Naja. 2020. "COVID-19 foreign influence campaigns Europe and the global battle of narratives.". European Parliamentary Research Service. URL: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)649367

BERTHON, Pierre R.; LEYLAND, F. Pitt. 2018. "Brands, Truthiness and Post-Fact: Managing Brands in a Post-rational World". Journal of Macromarketing 38, No 2.

BITTMAN, Ladislav. 1985. The KGB and Soviet Disinformation: An Insider's View. Pergamon.

BOBBA, Giuliano. 2017. "Social media populism: features and 'likeability' of Lega Nord communication on Facebook", European Political Science. Vol. 18. 11-23. DOI: 10.1057/s41304-017-0141-8

BOZDAG, E. 2017. "Bias in algorithmic filtering and personalization". *Ethics and Information Technology* 15, 209–227. DOI: https://doi.org/10.1007/s10676-013-9321-6

CAMERON, Martel; PENNYCOOK, Gordon; RAND, David G. 2020. "Reliance on emotion promotes belief in fake news". Emotions and fake news. URL: https://cogsci.yale.edu/sites/default/files/files/2020ThesisMARTEL.pdf

CERVI, Laura; GARCÍA, Fernando and MARÍN-LLADÓ, Carles. 2021. "Populism, Twitter, and COVID-19: Narrative, Fantasies, and Desires". Social Sciences 10. DOI: https://doi.org/10.3390/socsci10080294

CINELLI, M., Quattrociocchi; W., GALEAZZI, A. et al. 2020. "The COVID-19 social media infodemic." Scientific Reports 10, 16598 (2020). DOI: https://doi.org/10.1038/s41598-020-73510-5

CITRON, Danielle K.; CHESNEY, Robert. 2018. "Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?", Lawfare. URL: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship

DASCĂLU, Ștefan; GEAMBASU, Oana; COVACIU, Ovidiu; CHERECHES, Razvan Mircea et al. 2021. "Prospects of COVID-19 Vaccination in Romania: Challenges and Potential Solutions", Public Health. DOI: ://doi.org/10.3389/fpubh.2021.644538

FAKHRUDDIN, B.; BLANCHARD, K.; RAGUPATHY D. 2020. "Are we there yet? The transition from response to recovery for the COVID-19 pandemic". Progress Disaster Science, 100102 (2020), DOI: 10.1016/j.pdisas.2020.100102

FUNKE, Manuel; SCHULARICK, Moritz; TREBESCH, Christoph. 2020. "Populist leaders and the economy", ECONtribute Discussion Paper, No. 036, University of Bonn and University of Cologne, Bonn and Cologne: Reinhard Selten Institute (RSI).

GERBAUDO, Paolo. 2018. "Social media and populism: An elective affinity?". Media, Culture & Society 40: 745–53.

GREIFENEDER, Rainer; JAFFÉ, Mariela E.; NEWMAN, Eryn J.; SCHWARZ Norbert (Eds.). 2021. The Psychology of Fake News. Accepting, Sharing and Correcting Misinformation. London and NY: Routledge.

GUNNERIUSSON, Håkan. 2021. "Hybrid warfare: Development, historical context, challenges and interpretations." ICONO 14, Revista de comunicación y tecnologías emergentes, vol. 19, no. 1, pp. 15-37. DOI: https://doi.org/10.7195/ri14.v19i1.1608

HORSLEY, Jamie P. 2020. "Let's end the COVID-19 blame game: Reconsidering China's role in the pandemic." Brooking. URL: https://www.brookings.edu/blog/order-from-chaos/2020/08/19/lets-end-the-COVID-19-blame-game-reconsidering-chinas-role-in-the-pandemic/

HUNTINGTON, Samuel P.; DUNN, Steve. 2004. Who are We?: The Challenges to America's National Identity. London: Simon & Schuster.

JENTE, Althuis; HAIDEN, Leonie (Ed.). 2018. Fake News: A Roadmap, Riga: NATO Strategic Communications Centre of Excellence.

KHALDAROVA, Irina; PANTTI, Mervi. 2016. "The narrative battle over the Ukrainian conflict." Journalism Practice. DOI: 10.1080/17512786.2016.1163237

LAKOFF, George, JOHNSON, Mark. 1980. The Metaphor we live by. University of Chicago Press.

LEIGHT, Michael. 2021. "Vaccine diplomacy: soft power lessons from China and Russia?". Bruegel. URL: https://www.bruegel.org/2021/04/vaccine-diplomacy-soft-power-lessons-from-china-and-russia/

LIBICKI, Martin C. 2007. Conquest in Cyberspace National Security and Information Warfare. Cambridge University Press.

MALY, Ico. 2020. "Algorithmic Populism and the Datafication and Gamification of the People by Flemish Interest in Belgium", Trab. Ling. Aplic., Campinas, n (59.1): 444-468, Jan./Abr.

PARISER, Eli. 2011. The Filter Bubble: What The Internet Is Hiding From You. Penguin Books.

PARK, Andrew; MONTECCHI, Matteo; FENG, Cai 'Mitsu' et al. 2020. "Understanding Fake News: A Bibliographic Perspective" Defence Strategic Communications, Volume 8, (Autumn 2020), 141-172. DOI 10.30966/2018.RIGA.8.4

Reuters. 2020. "False claim: Picture shows people dying of coronavirus in the streets." Reuters. March 28, 2020. https://www.reuters.com/article/uk-factcheck-coronavirus-art-performance-idUSKBN21F05U

RIDLEY, Anne M.; GABBERT Fiona; LA ROOY, David J. (Eds.). 2013. Suggestibility in Legal Contexts: Psychological Research and Forensic Implications. John Wiley & Sons.

SAEZ-TRUMPER, Diego. 2019. "Online Disinformation and the role of Wikipedia". ArXiv, URL: https://arxiv.org/pdf/1910.12596.pdf

SERRANO, Raquel Miguel; ADAMCZYK, Roman; SESSA, Maria Giovanna; Laurem HAMM. 2020. "COVID-19 Disinformation: Narratives, Trends, and Strategies in Europe." EU Disinfo Lab. URL: https://www.disinfo.eu/publications/COVID-19-disinformation-narratives-trends-and-strategies-in-europe/

VALÁŠEK, Tomáš (Ed.). 2018. New Perspectives on Shared Security: NATO's Next 70 Years. Washington: Carnegie Endowment for International Peace Publications Department.

VALENZA, Domenico. 2020. "The Irresistible Rise of Health Diplomacy: Why Narratives Matter in the Time of COVID-19". Institute on Comparative Regional Integration Studies". March 30, 2020. https://cris.unu.edu/health-diplomacy-narratives

WARDLE, C., DERAKHSHAN H. 2017. "Information disorder: Toward an interdisciplinary framework for research and policy making". Council of Europe Report 27. URL: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

World Health Organization. 2020. "COVID-19 mythbusters". URL: https://www.who.int/westernpacific/emergencies/COVID-19/information/mythbusters

YIQUAN, Gu and WENZEL, Tobias. 2014. "Strategic Obfuscation and Consumer Protection Policy" Journal of Industrial Economics, Wiley Blackwell, vol. 62(4).

DOI: 10.53477/2668-6511-22-13

CHALLENGES AND VULNERABILITIES OF EQUAL OPPORTUNITIES AND MIGRATION IN THE EUROPEAN UNION

Delia-Mihaela MARINESCU, Ph.D.,
"Carol I" National Defence University, Bucharest, Romania
E-mail: delia.marinescu@ymail.com

Abstract: *Respect for equal opportunities and control of migration are the basis for the development of any democratic society, the magnitude of these phenomena and their importance on the state balance determining an analysis consistent with the very identity of states and the European Union as a whole, especially as they can influence the values and cohesion of a state. The objective of the research is to present the challenges and vulnerabilities identified in relation to equal opportunities and migration from the perspective of education, their impact on the environment, but also the challenges that may arise in the current global context, caused by the Covid-19 pandemic. The article starts from the exposition of the importance of equal opportunities and migration in a complex security environment with rapid evolutions and significant implications on multiple levels of social, economic, political and security life, and the main conclusion is that at EU level joint efforts must be made to adopt and respect unitary measures to ensure respect for human rights, in order to ensure security.*

Keywords*: migration; equal opportunities; security; challenges; vulnerabilities; education.*

Introduction

In a complex, constantly evolving security environment, which aims at ensuring global stability and create effective structures in key areas of citizens' lives, strengthening resilience in education is one of the priorities of European policy indispensable for reducing vulnerabilities in the field, but also for the efficient management of current challenges, including the COVID-19 pandemic.

Ensuring the security of citizens at EU level (Commission Communication 2020 Strategy) and respect for fundamental human rights and freedoms can only be analyzed in close connection with a high-performing education system, based on respect for equal opportunities, but also on guaranteeing an effective access to education for migrants, especially given that migration is a reality of today's globalized world.

In the context of security generated by the COVID-19 pandemic, the education system in the EU has been severely affected, in the sense of fundamentally changing some coordinates of the learning process, which have had an impact globally, not only from the perspective of radically changing the way of delivery, which was for the first time faced with the challenge of running online, but also from a financial and logistical perspective, given the costs and technical resources required.

Therefore, a relevant analysis of respect for equal opportunities and the rights of migrants in education is needed to consider the challenges and vulnerabilities that may arise in this area in relation to the need to respect fundamental rights and freedoms, the values of the European Union, but also to ensure an efficient framework that can guarantee an adaptation of the existing system to the constantly changing practical realities.

1. Equal opportunities in education

As a fundamental right of every human being, education is the basis of a society's progress, guaranteeing respect for a state balance, which has led to increased attention at the European Union level, given the implications not only on the education sector itself, but also on the labor market, but also the vulnerabilities that can appear in the address of security, especially in the situation of the existence of some discriminations that can lead to inequities.

The analysis of vulnerabilities must have in the foreground the study of the quality of the educational act and the importance of investments in human resources in education, through European funding and by allocating sufficient amounts by Member States to train teachers, but also to create a suitable framework to facilitate the learning process for students, including through investments in digitization, which have become indispensable in the context of the Covid-19 pandemic and the impact it has had on the educational process.

Respect for equal opportunities in education, which is considered essential in the European Union but also worldwide, derives from its regulation not only at the level of the European Union, but also through international legal acts, such as the Convention on the Elimination of All Forms of Discrimination against women who rule in art. 10 the need to eliminate gender discrimination in education, the International Covenant on Economic, Cultural and Social Rights (International Covenant 1966,5) which guarantees in art. 13 the right of everyone to education, including those belonging to racial, ethnic and religious groups, as a basis for the development of a free society, but also the UNESCO Convention on Action against Discrimination in Education (UNESCO Convention 1960), which requires the adoption of each state of policies capable of ensuring the participation of all children in the educational process, without discrimination and with the recognition of the rights of minorities.

Fundamental value of the European Union, established by art. 2 of the Treaty on European Union, equality finds its applicability in all spheres of social life, constituting the basis for the development of a modern society and imposing on the Member States a positive obligation (Rădulescu 2021, p.3) to ensure an adequate framework for implementing policies.

Equal opportunities in the field of education at European level is regulated specifically by art. 14 of the Charter of Fundamental Rights of the European Union which guarantees the right of any person to education, but also to access to vocational training, these provisions complementing the principle established by art. 21 of the same normative act that generically prohibits discrimination, for any reason.

In this regard, the Council adopted the Strategic Framework for European Cooperation in Vocational Education and Training -ET 2020- which sets as its basic objective the observance of equity and social cohesion in education, so that "all citizens, regardless of personal circumstances , social or economic development, to develop lifelong skills specific to the profession", being applicable to any form of education, including that of adults, the principle being found in the Declaration on the Promotion of Citizenship and the Common Values of Freedom, Tolerance and non-discrimination through education (Promoting citizenship, 2015) that promotes gender equality in education.

It should be clarified that Member States have competence in the field of education, setting guidelines related to national specificities, but the role of the EU, which provides funding and support, cannot be neglected in order to guarantee a framework to ensure investment. efficient in human capital, but also an active involvement in the development of education in areas with difficult economic situation.

The connection between equal opportunities and education must be analyzed both from the perspective of equal access to education for all, without discrimination, and the professionalization of teachers in the spirit of respecting and understanding these concepts in order not to create differences in the educational process chosen in the conditions in which a

low quality of the educational act and the existence of discriminatory elements in the field can constitute vulnerabilities to security.

Thus, the European Union made considerable efforts during the COVID-19 pandemic to maintain and strengthen a European area of education (Commission Communication Space 2020) with a focus on both the development of the digital sector and the promotion of an interdisciplinary education policy, including on promoting intercultural education which is indispensable for the progress of states and which cannot be dissociated from respecting diversity and accepting the idea of preserving the values and culture specific to each group and whose non-compliance can be a vulnerability in the context of today's globalized society.

At European Union level, several programs have been adopted to lay the foundations for increased performance in schools in the Member States, with a focus on preventing early school leaving (Eurydice Report 2019, 31) which is a real problem, especially in rural areas, which makes it necessary to implement programs to provide grants for people from disadvantaged backgrounds, including both logistical support for the educational process, such as textbooks, supplies, and social scholarships.

In this sense, it is necessary to specify the Erasmus program, which is applicable in all European Union countries and which is important in respecting mobility in the European space, by ensuring the right of everyone to social inclusion, but also to cooperation in education and in vocational training, by promoting a quality education that ensures the premises for the social integration of the beneficiaries and for the economic development of the society.

The education system is based on respect for and promotion of human rights, so equal access to education must be presented in terms of respect for equality, as the basis for effective integration into society and access to employment, which ensures the maintenance of social security, taking into account and the fact that the main causes of inequalities in the education system are based on socioeconomic differences, deterioration of living conditions, including differences between educational institutions regarding the quality of education, or concrete learning conditions (Neagu 2009, 76).

Regarding the identification of potential challenges that could arise in respecting equal opportunities in education, it is necessary to mention first of all the need to correlate public education policies and reform policies adopted with the actual needs of the system and with the implementation of measures to ensure a predictability at least in the medium term in order not to generate disturbances in the educational process.

The importance of respecting equal opportunities in education must also be analyzed in relation to information campaigns carried out mainly at the level of teachers, in order to explain the need to apply the principle of equality in education and to be aware that the risks of non-compliance may affect long-term and not only at the level of the education sector, but also affects all spheres of social life, especially since the existence of forms of discrimination is an interference with respect for human rights.

The schooling of a child must be based on creating all the prerequisites for providing opportunities for integration into the labor market, by providing free access to any type of career option, according to skills. Education is the foundation of any citizen's development, it is a real challenge, including emphasis on the fact that education must not be seen only in terms of completing the compulsory stages of schooling, but is an ongoing process, which is indispensable in professional activity.

In discussing the challenges to equal opportunities in the field of education, it is necessary to take into account the factors that lead to inequities, which are so subjective and related to the social environment of the student, the entourage, the cultural-educational level of the family, as environment in which a child grows up and is trained for life (Bădoi, Mateiescu 2016, 26), financial resources as well as objective ones, such as those related to the distance

from the school in the case of children from disadvantaged areas, they must be taken into account in developing the state policy in order to implement the curriculum related to the possibilities of children, but also to ensure sufficient funding and implementation of programming through which objective impediments can be eliminated.

In conclusion, in applying the principle of equal opportunities in education, both vulnerabilities and challenges can be identified, and it is essential to correlate state policy with the concrete and particular situation of each Member State of the European Union, especially given that the educational process occupies a significant part in each person's life and has long-term effects, not only on the information needed for schooling, but also on the implementation of principles of life that are in the spirit of European values and respect for human rights.

Thus, equal opportunities in education are not limited to the analysis of respect for gender equality, non-discrimination in relation to criteria such as ethnicity, religion or nationality, but extends to society as a whole, including the impact on economic fields, socially or politically, the existence of cases of discrimination having effects on maintaining state societal security, so that the emergence of vulnerabilities and challenges in this area is increased.

2. Immigrant education

States facing a significant influx of immigrants must ensure a functional framework for their effective integration into the host society and for ensuring access to an education system that facilitates their access to the labor market, as a key aspect of accelerating the process of integration (Avram 2019,87), which can be a real challenge to security, especially given that education is the main means of adaptation in the new state, which can help establish lasting social relations in the community.

In European countries, it is necessary to organize the education system in order to facilitate the access of all immigrants to education and vocational training and to ensure the provision of the necessary knowledge and the provision of sufficient skills to try to effectively guarantee them equal opportunities in society with those of the citizens of that state and to constitute a real guarantee against discrimination (Rădulescu 2021,143), especially taking into account the fact that students from migrant families face challenges related to the migration process, the socio-economic context and general policy or the way in which students participate in education, which does not always take into account both school and non-school aspects that may affect their education and development (European Commission Integration of Students 2019, 9).

Currently more than 34 million people are born outside the European Union (Communication Commission Action Plan 2020.2) and more than a quarter of them have higher education (Idem Plan 2020) at the time of leaving the country of origin, but are few people manage to capitalize on their previous professional training in finding a job that matches their studies, most of them either working in fields that do not require a higher qualification, or in areas of activity completely different from their training.

Immigrants go through an educational process giving them an extra chance to integrate into the host state, the proportion of effective integration being even higher as access to education takes place at an earlier age for children, which increases hopes for access to higher positions in society for migrants, which was the premise for leaving the country of origin, in search of a higher standard of living and a better life.

The real challenge for children from migrant backgrounds is to have school results similar to those of native children, especially as they start with a deficit caused by a lack of sufficient financial resources to facilitate their access to a successful education system, possible shortcomings in the educational system of the families of origin, but also in the insufficient

resources allocated by society to combat inequalities in the educational process, aspects that diminish as more generations of migrants live in the host country and which can accentuate sentimentally the lack of membership in the host state. Thus, in France, for example, the persistence of the gap between children of the second generation of immigrants and those of the indigenous population contradicts predictions of intergenerational mobility based on educational and social progress in this regard (Meurs, Pailhé, and Simon 2005, 1) which indicates a process of educational discrimination over a long period of time, thus affecting even the descendants of immigrants born and raised in the host country.

These situations make it difficult to integrate into society, especially from the perspective of the deficiencies of deepening the language of the host state, which can be a factor of intimidation for immigrant students, but also a barrier in adapting to the new community, which led to the need to implement policies at European level to focus on the integration of migrants in the host countries, but also on the assessment of the situation, in relation to the skills acquired by them, given that completing an educational cycle in the host state provides the preconditions for obtaining a job obtained through studies, taking into account the aspirations of students, but also the respect for equality in the labor market.

The difficulties of integration into the education system of the detination country and the constant challenges faced by European countries with a large influx of immigrants have generated the need to implement exchanges of good practice aimed at monitoring the school situation of immigrant children, including performance their education in the countries of origin, if the child has previously completed stages of schooling in that country, but also in the integration into the new state, with the analysis of respect for intercultural dialogue, but also for linguistic and cultural diversity (Eurydice Report 2019, 16).

The importance of the educational act, as a vulnerability to security, must also be analyzed in terms of ensuring greater attention in favor of children from migrant families in order to guarantee, on the one hand, the existence of equality in the education process and, on the other , further integration into the labor market, given that the needs of migrant children are higher than those of children of native parents in the host country, taking into account economic and social disparities, which may lead to the need to adapt curricula to their needs.

In this context, an important role can be played by the actions taken by society to advise migrant students, but also to train teachers to facilitate the integration of these children in the community, respecting their own culture and traditional values in the country of origin. The lack of attention to these aspects can lead to dropping out of school and to social exclusion, given the fact that the educational process of migrants is a complex one.

At EU level, challenges in the field of immigrant education can be identified mainly in countries facing significant migratory flows and which are an attraction even for students accessing mobility programs, such as Erasmus, which target higher education people who want to benefit from an exchange of experience with partner universities from other states and to access the educational system of another state, which is culturally and linguistically different, in order to benefit from an international educational experience.

In the same vein, the School Education Gateway portal has been set up, which is subsidized by Erasmus + and which facilitates students from other countries to access information materials and exchange information that will allow them to be more easily included in the host state, with ensuring the cultural diversity and values of each community, but also the eTwinning Platform (eTwinning) which offers teachers the opportunity to present their experiences of interaction with migrant children, in order to facilitate their integration, including in terms of language differences.

In addition, another real challenge facing immigrants in the education system is the language difficulty in the host country. This aspect can be a negative point in the educational

process and can be a determining factor for school dropout, given that the emphasis at the social level is not on the development of intercultural dialogue, as a basis for the integration of migrants in the host state. It is therefore necessary to adopt language training programs prior to integration into the compulsory education system in order to eliminate situations in which immigrants feel harassed by native students, which creates a feeling of discrimination, language differences can be an important factor to generate a state of intimidation and generate a lower sense of belonging to the school.

At the level of EU decision makers and Member State decision-makers, it is necessary to adopt policies for the protection of immigrant children and to guarantee their effective equal access to education, both in relation to other migrants and to the natives of the host state, so that there is no risk that in fact the children of immigrants will not be able to benefit from the same educational conditions, which would generate an inequality of cognitive development.

Thus, since 2016, the European Commission has supported EU Member States in their efforts to integrate migrants into their education and training systems - from pre-school education and care to higher education, the Commission's Action Plan on Integrating Third-Country Nationals (Commission Plan 2016,8-9) developed for this purpose focusing on several priority directions such as the integration of newly arrived migrants in general education structures as soon as possible, the possible prevention of poor school results among migrants, as well as the prevention of exclusion and the promotion of intercultural dialogue.

In addition, access to education must be effective at both compulsory and post-compulsory schooling, which can allow the exploitation of the intellectual potential of each student, but also his concrete skills that will allow him to find a job in conditions. similar to a native, adapted to professional training and skills, which is a real challenge for the host state to adopt a legislative framework in this regard and to sanction legally or jurisprudential cases of violations of the principle of equality in this area.

Given that education and migration have been among the most affected by the Covid-19 pandemic, they can continue to pose multiple challenges and vulnerabilities, which can affect security and involve rapid and effective action by state authorities, on the one hand, to guarantee real access to education for all social categories, targeting both natives and immigrants, and, on the other hand, to ensure access to the labor market for effective social integration in the host state.

Conclusions

Education is one of the key areas of state security, which involves the adoption of resilient policies that ensure cooperation between the states of the European Union, given the interdependence in the implementation of coordinated measures to reduce vulnerabilities in the field and deal effectively with challenges, which are more and more numerous, also taking into account the Covid-19 pandemic.

In this context, the identification of vulnerabilities and challenges related to education are the initial prerequisites for guaranteeing equality and for their efficient management, in the sense of adopting legal measures to reduce the risk of affecting the security of states and the EU as a whole, being indispensable a common action of the institutions of the European Union and of the Member States in this respect.

The present paper identifies as main vulnerabilities in the field of education those related to: the low quality of the educational act that can generate discrimination and social inequities with the violation of equal opportunities; undervalued investments in the field of human resources in relation to teacher training and digitization investments strictly necessary during the pandemic COVID-19 and the existence of a deficient and unequal educational process, violating the values and culture of each group of immigrant children with effects negative for

their full integration into European values, which accentuates the feeling of discrimination and belonging to the host state.

The challenges analyzed in the paper are multiple but, mainly, refer to the identification of the best solutions for the correlation of public policies in education and reform policies; ensuring predictable medium-term measures in education; ensuring the institutional and organizational framework for the learning activity to be a continuous process, including in the professional activity in the spirit of European values; Elimination of subjective and objective factors that lead to inequities in education; ensuring a functional framework for the rapid integration of immigrants into host societies and their access to an equal and effective education and training system that provides the knowledge and skills necessary for development within that society; respect for intercultural dialogue and linguistic and cultural diversity; combating school dropout and social exclusion of immigrants as well as providing them with intensive training programs for language learning in the host country.

Respecting equal opportunities and controlling migration through the implementation of measures to ensure that the rights of immigrants in the host state are respected are some of the most difficult aspects to manage in today's globalized society, where it is essential to guarantee diversity in all respects and non-discrimination access to employment, on equal terms for all, including natives.

BIBLIOGRAPHY:

AVRAM, Lucia-Ştefania. 2019. „Imigrația și integrarea migranților", article published in Revista *Universul Juridic*, no. 3, March. URL: http://revista.universuljuridic.ro/wp-content/uploads/2019/05/08_Revista_Universul_Juridic_nr_3-2019_PAGINAT_ BT_L_Avram.pdf

BĂDOI, Mădălian Ionela; MATEIESCU, Bianca Elena. 2016. „Provocările actuale ale educației și problemele tinerilor între formare și integrare", article published in *Analele Universităţii "Constantin Brâncuşi"* din Târgu Jiu, Seria Ştiinţe ale Educaţiei, No. 1/2016. URL: https://www.utgjiu.ro/revista/dppd/pdf/2016-01/3_Sorin-Avram%20 VIRTOP,%20Madalina%20Ionela%20BADOI,%20Bianca%20Elena%20 MATEIESCU.pdf, accessed on 27.09.2021.

Buletinul Oficial nr. 146. 1974. *International Covenant of 16 December 1966 on economic, social and cultural rights.* URL: http://legislaţiei.just.ro/Public/Detalii DocumentAfis/82589

Commission action plan on integrating third-country nationals, 2016. Strasbourg, COM(2016) 377 final, URL: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX: 52016DC0377&from=RO

Commission on the EU Security Union Strategy. 2020. Communication, Bruxelles, URL: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020DC0605 &from=RO

Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the achievement of the European Education Area by 2025. 2020. Communication, URL: https://eur-lex.europa.eu/legal-content/ RO/TXT/HTML/?uri= CELEX:52020DC0625&from=EN

Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan on Integration and Inclusion for the period 2021-2027. 2020. Communication, Bruxelles. URL: https://eur-

lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0758&qid=1616495531813&from=EN

MEURS, D., PAILHE, A. and SIMON, P. 2005. *Mobilité intergénérationnelle et persistance des inégalités : l'accès à l'emploi des immigrés et de leurs descendants en France*, Paris, INED. URL: https://www.ined.fr/fichier/s_rubrique/19404/130.fr.pdf

NEAGU, Gabriela. 2009. *Măsurarea şanselor de acces la educatie*, în Paradigma calităţii vieţii, capitolul 3, Editura Academiei Române, URL: https://www.researchgate.net/publication/268149888_Masurarea_sanselor_de_acces_la,_ educatie

Publications Office of the European Union. 2015. *Promoting citizenship and the common values of freedom, tolerance and non-discrimination through education. Overview of education policy developments in Europe following the Paris Declaration of 17 March 2015*, URL: https://op.europa.eu/en/publication-detail/-/publication/ebbab0bb-ef2f-11e5-8529-01aa75ed71a1

RĂDULESCU, Dragoş-Lucian. 2021. *Raporturile juridice de muncă. Discriminarea multiplă*, Editura Didactică și Pedagogică, București.

The European Commission/EACEA/Eurydice. 2019. *Integrating pupils from migrant families into European schools: national measures and policies*. Raport Eurydice. Luxemburg: Union Publications Office. URL: https://op.europa.eu/en/publication-detail/-/publication/39c05fd6-2446-11e9-8d04-01aa75ed71a1/language-ro/format-PDF

The European Commission/EACEA/Eurydice. 2019. *Integrating students from migrant families into schools in Europe: national measures and policies*. Raport Eurydice. Luxemburg: Union Publications Office. URL: https://op.europa.eu/en/publication-detail/-/publication/ 39c05fd6-2446-11e9-8d04-01aa75ed71a1/language-ro/format-PDF

The official website of Eurydice, URL: https://eacea.ec.europa.eu/national-policies/eurydice/content/national-reforms-school-education-56_ro

The official website of the eTwinning Platform, URL: https://www.etwinning.net/ro/pub/index.htm

The official website of the School Education Gateway portal, URL: https://www.schooleducationgateway.eu/en/pub/index.htm

UNESCO. 1960. Convention on Combating Discrimination in Education. URL: http://irdo.ro/irdo/pdf/087_ro.pdf

DOI: 10.53477/2668-6511-22-14

ROMANIA IN THE NEW SECURITY ENVIRONMENT AFTER THE 2021 BRUSSELS SUMMIT

Raul NISTOR,
Lieutenant, Master student at the Faculty of Political Science
"Global Security Studies" of the West University of Timișoara, Romania.
E-mail: n.raul_nistor@yahoo.ro

Abstract: *The recent actions of the Russian Federation have raised major concerns among the Euro-Atlantic community. At a time when the security environment we face is becoming increasingly complex, at the NATO Summit in Brussels in 2021, member states reaffirmed their unity, solidarity, cohesion and agreement to open a new chapter in the transatlantic relations. At the same time, NATO remains the foundation of collective security and the essential forum for security consultations and decisions between allies. Romania will also play an extremely important role on NATO's vulnerable south-eastern flank, in the face of the Russian Federation's offensive. Thus, we aim to evaluate the place and role that Romania has as a contributing member of the alliance in ensuring security.*

Keywords: *Russian Federation; NATO; Romania; summit; deterrence and defence; security environment.*

Introduction

The Russian Federation is a revisionist state (Hudson Institute 2015). However, the Soviet Union appeared to be a revisionist power for the first time since World War II in 1990, when President Mikhail Gorbachev's view of post-Cold War Europe's collective security system was not shared by the Euro-Atlantic community. The Soviet Union became dissatisfied, as its opinion was not taken into account, and it could not have a voice in the post-Cold War European security environment that included NATO (North Atlantic Treaty Organization) and the EU (European Union) as main actors (Diyarbakirlioglu 2019, 4). Thus, the Russian Federation seemed to be a potential revisionist state starting with the collapse of the Soviet Union, but it really became one in 2007, with the speech held in Munich (President of Russia 2007), by creating the framework of the "Russian World" (Ukraine Crisis Media Center 2021) and suspending The Conventional Armed Forces in Europe (CFE) Treaty (Radio Free Europe 2007). All this happened after the Colour Revolutions in Georgia in 2003 and Ukraine in 2004 and also after the enlargement of NATO and the EU to Eastern Europe in 2004, through the review of the defence and security policy of the Russian Federation by Vladimir Putin.

In fact, the enlargement of NATO and the EU has posed a threat to the traditional sphere of influence over the former Soviet Union and a challenge to the authoritarian regime in the Russian Federation, as Euro-Atlantic diplomacy promotes values such as democratization, the rule of law and the market economy. These values promoted by NATO and the EU have led to internal conflicts within the former Soviet republics of Georgia and Ukraine. These conflicts simply posed a threat to the Russian Federation, and could eventually spread within the borders of the Russian Federation.

Therefore, with the start of his second term, the Russian president has developed a more assertive foreign and security policy and focused on the dispute with NATO and the EU over

the former Soviet republics, now independent, and the South Caucasus states. Subsequently, after the NATO Summit in Bucharest in 2008, after Ukraine and Georgia received guarantees for possible NATO integration, the Russian Federation changed its policy of ensuring the integrity of Georgia's territory and decided after the Russian-Georgian War took place in August 2008, to officially recognize the independence of the separatist republics of Abkhazia and South Ossetia (Radio Free Europe 2008). Subsequently, in March 2014, the Russian Federation annexed the Crimean Peninsula and began supporting the secessionist movement in eastern Ukraine. Thus, the Russian Federation has obviously become a revisionist state, making the first annexation of the 21st century, and the Euro-Atlantic community has imposed sanctions to it, but without notable results.

1. Romania and NATO in the new security environment

The strategic trends in recent years illustrate the accumulation of a substantial potential to reconfigure the relations between actors with global interests, with direct effects on the stability and predictability of the international system, and the revitalization of global strategic competition confirms the transition to a new security paradigm. This will accentuate the tendency towards a more sustained activity of the states in bilateral plan, with momentary and conjectural interests and alliances, which will affect even more the predictability of the international security environment (Administrația Prezidențială a României 2020, p. 17). The current security environment is characterized by a high degree of dynamism and unpredictability, as well as by the increased globalization of threats and risks, with various manifestations and unlimited potential for geographical spread (Administrația Prezidențială a României 2020, p. 19).

As a state on the eastern flank of NATO and on the eastern border of the European Union, the main vectors for promoting stability and security for Romania are the national capacity and membership to these organizations. Both have proven their ability to effectively meet their objectives of ensuring the security and economic prosperity of the Member States, while demonstrating a strong strategic potential for permanent adaptation to changes in the security environment (Administrația Prezidențială a României 2020, p. 21).

Prior to joining the select club of NATO member states in 2004, Romania sought this goal for a long time, starting with the end of the Cold War. During the accession process, the former Romanian Chief of Defence, General Constantin Degeratu, stated "it is fair to say that no state has led a more aggressive NATO accession campaign than Romania. As Romania cannot claim leadership values in terms of democratization and economic reforms, it has highlighted its strategic location (Puri, n.d., p. 1)."

A decade after Romania joined NATO in March 2014, to the surprise of the international community, the Russian Federation annexed Crimea, violating a whole set of fundamental principles of international law and other treaties that guarantee territorial integrity, inviolability of borders and security to Ukraine (Merezhko 2015). The attitude and actions of the Russian Federation, in violation of the rules of international law, generate the perpetuation and expansion of differences with some Western states and NATO, constituting serious obstacles in identifying viable solutions to ensure stability, predictability and security (Administrația Prezidențială a României 2020, p. 17).

Due to the bringing back to the forefront of Romania as a state bordering the Black Sea, by accepting it in the alliance, NATO expanded its opening to the Black Sea, at the same time Romania becoming part of the south-eastern flank of NATO. Also, the conflict in eastern Ukraine triggered a sharp deterioration in relations between the Russian Federation and the West, but from Romania's perspective, the presence of a regional hegemony of the Russian Federation meant a permanent concern. Thus, the constant actions of the Russian Federation to

strengthen its offensive military capabilities in the Black Sea and to create a system of regional interdiction and restriction of access. This will ensure control over the Pontic basin and counterbalance the development of Allied military capabilities on the eastern flank of the NATO. It demands a consolidated national defence position and the continuation of Romania's active attitude in order to consolidate the allied posture of deterrence and defence in the region (Administrația Prezidențială a României 2020, p. 22).

By bringing back to the fore the objective of discouraging the Russian Federation, NATO has really come close to the concerns of its members on the south-eastern flank, including Romania. Romania's geography and history reflect the fact that it must always pay special attention and concern to a dominant and revisionist Russian Federation. Thus, according to Robert D. Kaplan the experience of the communist period as a repressive regime, determined Romania to deeply desire its integration in Western formats such as the EU and NATO. Romania and NATO's objectives of discouraging the Russian Federation converge, as well as Romania's national security calculations, namely to counterbalance the military power of the Russian Federation in the Black Sea, on the same side of the barricade, together with the United States of America (USA) and with Western European states. Therefore, for Romania, the Black Sea region represents an area of maximum strategic interest (Administrația Prezidențială a României 2020, p. 21).

Thus, the potential for escalating tensions in the region, amid the strengthening of the offensive position and the aggressiveness of the Russian Federation in recent years and the improvement of the hybrid instruments it uses, is a major security concern in the national context. From this perspective, strengthening the Alliance's deterrence and defence posture, especially on its eastern flank, through a united north-south approach, enhancing the EU's capacity to act together and the US commitment to the security of the Black Sea region are key elements and sustainable solutions to ensure regional stability. For Romania, it remains a priority to reconfirm the relevance of the Black Sea, with strategic importance in the regional security configuration. That is why, in a dynamic security environment with a high degree of unpredictability, adapting the narrative used to maintain and increase the US, NATO and EU attention on the strategic importance of the Black Sea is a permanent and important process for the country (Administrația Prezidențială a României 2020, p. 22).

2. Romania's objectives for the 2021 Brussels Summit

In terms of defence and national security, the Supreme Council of National Defence (CSAT) is the authority responsible for these activities. Procedurally, before the NATO Summit takes place, NATO staff sends a draft of the final statement to the Ministry of Foreign Affairs. Subsequently, the Ministry of Foreign Affairs redistributes this document to state institutions that are part of the CSAT (Presidential Adviser for National Security, Minister of Defence, Minister of Internal Affairs, Minister of Foreign Affairs, Minister of Justice, Minister of Economy, Minister of Entrepreneurship and Tourism, Minister of Finance, Director of the Romanian Intelligence Service, Director of the Foreign Intelligence Service, and Chief of Defence) (Consiliul Suprem de Apărare a Țării 2002). In the first phase, these state institutions evaluate, analyse and make proposals, and after that, CSAT verifies and establishes the main objectives that Romania must support and achieve during the summit.

Therefore, in April, during the CSAT meeting organized in the context of the accumulation of Russian Federation troops on the eastern border of Ukraine, the security situation in the Black Sea region was analysed. In addition, during the meeting of the CSAT, it was decided that, on the NATO line, Romania will continue to promote the steps meant to

lead to the further consolidation of the allied position in Romania and in the region (Consiliul Suprem de Apărare a Țării 2021).

Subsequently, at the special meeting of the Foreign Ministers of NATO countries, held in video-conference format, whose main objective was the preparation of the NATO Summit on June 14, the Romanian Minister of Foreign Affairs, Bogdan Aurescu, pleaded for the consolidation of the NATO deterrent position in the south of the Eastern Flank and for a massive increase in the Allied presence on the Black Sea. In addition, he called for increased support for NATO partners. Bogdan Aurescu stressed that the measures are necessary in the current context of security in the East, which is marked by Russia's recent actions in the region, including those related to Ukraine, and against the background of its military consolidation in the Black Sea and support for Belarus (Bolocan 2021).

Another important event, which had the role of preparing the ground for the negotiations for the NATO Summit in June, is the B9 Summit in Bucharest in May. The Bucharest Format (B9) is an initiative launched by the President of Romania, Klaus Iohannis, and the President of the Republic of Poland, Andrzej Duda, in which NATO member states on the Eastern Flank of the Alliance take part: Bulgaria, Czech Republic, Estonia, Latvia, Lithuania, Poland, Romania, Slovakia and Hungary (Lupitu May 11, 2021). Romanian President Klaus Iohannis announced at the end of the Summit in a joint press conference with his Polish counterpart, Andrzej Duda, that: "The worrying security situation in the Black Sea has shown us that we must remain vigilant. Therefore, NATO must continue to strengthen its position of deterrence and defence, especially on the Eastern Flank, in a unified and coherent manner, from the Baltic Sea to the Black Sea. That is why I pleaded – including in the discussion with President Biden – for an increase in the Allied military presence, including the USA, in Romania and in the south of the Eastern Flank" (Lupitu May 16, 2021).

Therefore, a priority of Romania's objectives at the NATO Summit in June also seemed to be the attempt to correct the inequality manifested by NATO's defence and deterrence strategy between the north and south of NATO's eastern flank.

3. Romania's results at the NATO Summit in Brussels

As I mentioned before, the Black Sea became a hot sea after 2014, when Russia annexed Crimea, supplemented the military arsenal in Sevastopol and started the conflict in Donbas. New battleships were brought to Novorossiysk and Crimea; missiles were mounted that could reach the Romanian shore of the sea or target the Bosphorus.

Worryingly, the Euxinus Pontus has become a large ammunition and weapons depot, a dangerous place where territories can be snatched from what Russia calls its close neighbourhood, so spaces that were part of the Soviet Union until 1991. Ukraine is the first to be targeted, after Abkhazia and South Ossetia were taken from Georgia and Transnistria from the Republic of Moldova. Moscow sent 100,000 soldiers and fighting vehicles to Ukraine's eastern border two months ago, trying to prove once again that it will not allow the country to join the West.

In this context, Romania managed to impose in the final document of the NATO summit in Brussels a series of extremely important issues in the economy of its national security and the security of the eastern flank of NATO and the EU.

Firstly, the strengthening of the NATO's deterrence and defence posture. That is, the presence of NATO troops in the region, in the context of threats from Russia, generously cited in the document. The credible and effective stance invoked in defence and deterrence, especially on the Eastern Flank, means sufficient capabilities and troops to deal with any threat at any time. In addition, the Black Sea region is a region of strategic importance - based on the

wealth of mentions made in the document - while the document itself notes that, the security situation on the Black Sea remains worrying (Chifu 2021).

The Alliance is already present in Romania in key points. The South-East Multinational Brigade from Craiova has the mission to provide the training framework for subordinate and affiliated structures, as well as the command and control of a NATO operation type Article 5 - Collective Defence, to contribute to the territorial and population security on the Southeast Flank of the Alliance (NATO 2018). The Headquarters Multinational Corps Southeast in Sibiu and the Headquarters Multinational Division Southeast in Bucharest, destined for the Land Forces, represent Romania's substantial contribution to consolidating a credible posture of defence and deterrence on the eastern flank (Agerpress 2020).

The military base in Kogălniceanu hosts several hundred American soldiers and NATO pilots involved in the air police mission over the Black Sea and has the capacity to facilitate the transport of 2,000 soldiers and 3,000 tons of materials per day. The Ministry of Defence will invest 400 million euros for the expansion and modernization of this military base on the seafront for the safe and optimal operation of a squadron of multi-role aircraft, for defensive or offensive operations (Chirileasa 2021).

The Deveselu military base hosts the NATO anti-missile shield: an anti-ballistic radar equipped with 24 interceptor missiles. The system is operated and protected by 500 Romanian soldiers and civilians and 250 American soldiers. The air base at Câmpia Turzii, where the Americans promised to invest 130 million dollars to become a strategic point of the air operations carried out by the United States on the eastern flank of NATO.

The alliance is also present in Romania in pursuit of other strategic objectives. The NATO Center of Excellence in Oradea has trained in the over 10 years of activity about 1500 specialists in the field of intelligence and is the main provider of HUMINT expertise (intelligence from human sources) within the NATO military intelligence services. Euro-Atlantic Centre for Resilience, where 70 specialists and their cabinets will work, especially diplomats, civil servants and military along with Romanian or foreign experts.

Secondly, NATO puts more emphasis on its support for Moldova's integrity, democratic reforms and defence assistance. This reference is another success of Romania at the NATO summit in Brussels. The alliance calls on Russia to withdraw its troops forcibly stationed in territories belonging to Georgia, Ukraine and the Republic of Moldova and informs it that NATO will not return to normal relations with Moscow until it complies with its international obligations and demonstrates that implements international law (NATO 2021).

Finally, another key point supported by Romania is the reference, in the text published at the end of the summit, to the importance of the Euro-Atlantic Centre for Resilience recently inaugurated in Bucharest. With the help of this Centre, Romania wants to become a pole of excellence and a provider of expertise for the member states of NATO and the European Union, as President Klaus Iohannis said (NATO 2021).

Conclusions

Romania has struggled for years to convince the United States and NATO that it is a predictable and trustful partner and that the various misalignments/delays have been just road accidents. The Strategic Partnership with the United States and the major military investments made by the Americans in Romania determined Bucharest to be on Washington's side on every occasion. This includes NATO summits, where Western European states may have different views, suggesting, for example, more sovereignty and a partnership, not protectorate in the relationship with the USA.

Therefore, Romania represents an extremely important actor and ally for the eastern flank of NATO, which has adopted an active position in this period marked by tensions in the region, after the events of 2014. However, Romania still has a lot of work to do in order to be able to impose and promote its concerns about the security of the Black Sea region. The Russian Federation is a permanent concern for Romanian national security. Unfortunately, we appreciate that NATO does not assess these concerns of Romania at the same level, at the expense of other priorities of the alliance.

This paper has evaluated Romania's objectives at the NATO Summit in Brussels in 2021 and the wins of the efforts to convince the other NATO members regarding the importance of these objectives. In short, we recall the results of the analysis. First, NATO aims to strengthen the deterrence and defence posture. That is, the presence of NATO troops in the region, in the context of threats from Russia, which is generously cited in the final document. Second, after mentioning support for the sovereignty and territorial integrity of Ukraine, Georgia and the Republic of Moldova, the final communiqué notes NATO's very special support for democratic reforms in the Republic of Moldova. Third, the Summit set another goal for Romania, namely the need to increase resilience and maintain NATO's technological advancement. In terms of role, Romania is part of the efforts to increase resilience, by establishing and operationalizing the Euro-Atlantic Centre for Resilience (E-ARC).

However, it is imperative to mention the great failures of this Summit. The inequality in the way of giving importance to the northern part of the eastern flank compared to the southern part, which is clearly superior, has not been resolved even now. The inequality of NATO's security strategy between these two regions still continues and is reflected in the differences between the Enhanced Forward Presence in the Baltic States and Poland in the North and the Tailored Forward Presence in the South. In the text of the final communiqué, the neutral wording of the presence submitted is assumed. Unfortunately, there is no expected formula for a flank, an alliance, a single defence.

BIBLIOGRAPHY:

Administrația Prezidențială a României. 2020. "Strategia Națională de Apărare a Țării pentru Perioada 2020-2024". URL: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf

Agerpress. 2020. "HQ Multinational Corps South-East, established in presence of President Iohannis, DefMin Ciuca, in Cincu". URL: https://www.agerpres.ro/english/2020/07/23/hq-multinational-corps-south-east-established-in-presence-of-president-iohannis-defmin-ciuca-in-cincu--544875

BOLOCAN, Valentin. 2021. "România cere creșterea prezenței NATO la Marea Neagră: Putin are nevoie de scandal internațional ca să aibă liniște acasă". URL: https://adevarul.ro/news/eveniment/romania-cere-cresterea-prezentei-nato-marea-neagra-putin-nevoie-scandal-international-liniste-acasa-1_60b7a9135163ec4271b08bd0/index.html

CHIFU, Iulian. 2021. "Summitul NATO de la Bruxelles: Rusia rămâne principala amenințare a Alianței". URL: https://adevarul.ro/international/europa/summitul-nato-bruxelles-rusia-ramane-principala-amenintare-aliantei-1_60c831cc5163ec427119c6af/index.html

CHIRILEASA, Andrei. 2021." RO Army seeks contractor for EUR 400 mln project to modernize Kogalniceanu military base". Accessed September 28, 2021. https://www.romania-insider.com/kogalniceanu-base-modernization-march-2021

Consiliul Suprem de Apărare a Țării. 2002. "Legea nr. 415 din 27 iunie 2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării". URL: https://csat.presidency.ro/ro/prima-pagina/legea-de-organizare

Consiliul Suprem de Apărare a Țării. 2021. "Ședința Consiliului Suprem de Apărare a Țării din 27 aprilie 2021". URL: https://www.presidency.ro/ro/media/sedinta-consiliului-suprem-de-aparare-a-tarii1619532519

DIYARBAKIRLIOGLU, Kaan. 2019. "Russian and European Union's Quest for the formation of a European security system after the cold war". URL: https://www.tandfonline.com/doi/pdf/10.1080/23311886.2019.1683928?needAccess=true

Hudson Institute. 2015. "Putin's Russia as a Revisionist Power". URL: https://www.hudson.org/research/11386-putin-s-russia-as-a-revisionist-power

LUPITU, Robert. May 11, 2021. "Joe Biden, la summitul București 9 al aliaților de pe flancul estic: Susțin consolidarea capacității de apărare și descurajare a NATO în fața acțiunilor competitorilor noştri strategici". URL: https://www.caleaeuropeana.ro/joe-biden-la-summitul-bucuresti-9-al-aliatilor-de-pe-flancul-estic-sustin-consolidarea-capacitatii-de-aparare-si-descurajare-a-nato-in-fata-actiunilor-competitorilor-nostri-strategici/

LUPITU, Robert. May 16, 2021. "Klaus Iohannis l-a invitat pe Joe Biden la București. Ministrul Bogdan Aurescu: Prin participarea la summitul B9, președintele SUA a arătat că are încredere în România". URL: https://www.caleaeuropeana.ro/klaus-iohannis-l-a-invitat-pe-joe-biden-la-bucuresti-ministrul-bogdan-aurescu-prin-participarea-la-summitul-b9-presedintele-sua-a-aratat-ca-are-incredere-in-romania/

MEREZHKO, Oleksandr. 2015. "Crimea's Annexation by Russia – Contradictions of the New Russian Doctrine of International Law". URL: https://www.zaoerv.de/75_2015/75_2015_1_a_167_194.pdf

NATO. 2018. "Eight Allies join forces in Romania for Exercise SCORPIONS FURY 18". URL: https://www.nato.int/cps/en/natohq/news_160343.htm

NATO. 2021. "Brussels Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021". URL: https://www.nato.int/cps/en/natohq/news_185000.htm

President of Russia. 2007. "Speech and the Following Discussion at the Munich Conference on Security Policy". URL: http://en.kremlin.ru/events/president/transcripts/24034

PURI, Samir. n.d. "Romania: Black Sea Security and NATO's South-Eastern Frontline". URL: https://www.spf.org/projects/upload/Romania%2C%20Black%20Sea%20Security%20and%20NATO%E2%80%99s%20South-Eastern%20Frontline%20%28Puri%29.pdf

Radio Free Europe. 2007. "Russia Suspends Participation In CFE Treaty". URL: https://www.rferl.org/a/1079256.html

Radio Free Europe. 2008. "Russia Recognizes Abkhazia, South Ossetia". URL: https://www.rferl.org/a/Russia_Recognizes_Abkhazia_South_Ossetia/1193932.html

Ukraine Crisis Media Center. 2021. "Russkiy Mir" as the Kremlin's Quasi-ideology". URL: https://uacrisis.org/en/russkiy-mir-as-the-kremlin-s-quasi-ideology

DOI: 10.53477/2668-6511-22-15

NATIONAL LEVEL IMPLEMENTATION OF DIGITAL DIPLOMACY MECHANISMS AND FUNCTIONS BASED ON EU EXPERIENCE

Adrian Victor VEVERA, Ph.D.,
National Institute for Research and Development in Informatics – ICI Bucharest, Romania.
E-mail: victor.vevera@ici.ro

Abstract: *As information and communication technology has developed, its impact has been felt in many areas, including international relations. In the diplomatic field, changes have not been long in coming, while many European countries pioneering the use of the online environment to promote national interests and achieve foreign policy objectives. In this paper, we aim to highlight the main benefits of developing the field of digital diplomacy, the biases that the process has generated and to argue the urgent need to implement these technologies in Romania, based on existing experience in various EU countries.*

Keywords*: digital diplomacy; foreign policy; digitization; biases; international relations.*

Introduction

Digital diplomacy has begun to become a foreign policy desideratum of the 21st century, which means that the states of the world are trying to implement it as a foreign policy strategy and capitalize on its ability to influence and shape political agendas in critical areas of international relations. Following these trends, it is important for the European Union to implement digital diplomacy within the European Union's Common Foreign and Security Policy (CFSP) as a strategy for managing change in the international environment.

This implementation must aim to go beyond the sphere of public diplomacy, in the classical sense of the term, by capitalizing on the technologies that, in fact, signed the birth certificate of digital diplomacy – AI, big data, data mining, IoT, ML. Their inclusion determines the supplementation of the additional functions of diplomacy (representation, communication and negotiation) with new ones (creation and dissemination of knowledge) useful for identifying new ways to achieve foreign policy objectives. Firstly, the contribution of these technologies consists in generating a type of advanced knowledge of complex international contexts, which allows the identification of the most coherent scenarios for the evolution of the international environment and the establishment of the most relevant indicators. Thus, decision makers can make decisions with a higher degree of accuracy, in which there are valid variants of action/reaction depending on the transformations of the international environment.

This is a substantial change in the content of diplomacy, as it was traditionally understood, as it transgresses from a reactive field, which limits the effects of crises, threats, vulnerabilities or the potential for undesirable situations, an anticipatory field that can contribute to the establishment of a country on a desired path.

Through this article we aim to argue the need to design and implement a digital diplomacy strategy in Romania, based on both the literature and good practices already existing internationally.

1. Main Variables of the Digitization of Diplomacy Process

The versatility of information and communication technologies has led to the inclusion in the field of diplomacy of digital public diplomacy, e-governance, network diplomacy and cyber diplomacy. While the extensive use of digital technologies in different sectors of activity determines a serious increase of the digital vulnerability of the states, the cybernetic war became a reality that the national security of the states of our century is facing (Weiner 1996, 1).

The transformations that the field of diplomacy has undergone lately have determined the inclusion of the aspects generated by the use of ITC in the sphere of diplomacy taxonomy from the perspective of (Cull 2008):

1. changes caused by the use of ICT technology in the environment in which diplomacy takes place (geo-political, geo-economic, sovereignty, interdependence);

2. the emergence of new topics on diplomatic agendas (internet governance, cybersecurity, privacy and more);

3. the use of new tools (social media, big data and many others) offered by ICT technology in the practice of diplomacy.

The concept of digital diplomacy, which emerged as e-diplomacy, diplomacy 2.0 or twitter diplomacy, along with other associated concepts, has created an abundance of new terms, more or less overlapping, often confusing in implementing the political agendas of new forms. of diplomacy. Although the concept of digital diplomacy is still being clarified and developed, the *Cultural Diplomacy Dictionary* defines it as "a new form of public diplomacy, also called e-diplomacy, which uses the internet and new information and communication technologies as means for strengthening diplomatic relations. The main differences with the classical public diplomacy lie in a greater access to information, greater interaction among individuals and organizations, and greater transparency" (Chakraborty 2013).

The previous taxonomy indicates that cyber security is two-dimensional on the agenda of digital diplomacy as the advances in the digital field cannot be fully operational without addressing risks, vulnerabilities and opportunities of cyber space. 1. On the one hand, cyber security is becoming an intrinsic part of global phenomena such as cybercrime, information protection in the online environment, trust building, internet freedom and internet governance. These issues enter, by right, the area of manifestation of diplomacy, but through the complexity and specialization of the field has given rise to a new branch in the diplomatic field - digital diplomacy. 2. On the other hand, by implementing technologies specific to the field of information and communication, including activities continued under the auspices of traditional diplomacy (such as communication or negotiation between diplomats), they must use cybersecurity to ensure confidentiality in the online environment. Cyber security is intrinsically connected to phenomena such as cybercrime, confidence-building, internet freedom and internet governance. Both state-run personnel and diplomats can become victims of hackers, with the particular aim of obtaining confidential information that would serve purposes contrary to the interests of states.

The difficulty of protecting the digital environment has been understood by the UN, NATO, EU, OSCE, OECD, Commonwealth, G7 and G20, which have adopted a series of cyber security recommendations and strategies, doubled by relevant legislation. The EU adopted a cyber-security strategy – EU Cybersecurity Strategy, in 2013, on the basis of which, in 2015, the European Council adopted a special decision on cyber diplomacy - Council Conclusions on Cyber Diplomacy, thus marking a proactive role in the process of developing international cyber policies.

In this process, diplomacy has an important role to play in determining partnerships, building coalitions, maintaining human rights online and promoting equitable economic access.

Managing hybrid threats, in which cyber threats will always have a well-defined place, will be impossible in the absence of digital diplomacy.

The digitization of diplomacy occurred at the confluence of two major, apparently opposite trends determined by the emergence of new technologies:

1. The first mega-trend is the prerogative of skeptics and focuses on the costs of implementing new technologies in relation to their expected potential effects, considered to be incomparably lower;

2. The second mega-trend supports the implementation of new technologies and digitalization and encourages foreign ministries to take steps to facilitate and accelerate this process. Their haste is easy to understand given the pace of change today. If the landline phone took 75 years to reach 100 million users, the mobile phone needed 16, and the social network Facebook – only 4 and a half (Dreischmeier, Close & Trichet 2015);

Strangely, although they act concomitantly, the two trends do not cancel each other out and continue to gain followers and ground. Digitization is therefore dependent on a number of additional factors and variables, the existence / non-existence of which will induce a prevalence of one of the above trends or another.

Therefore, the discussion on digitization should consider at least the context, process and structure of the digital transformation of diplomacy.

1.1. The context of innovation in diplomacy

If we analyze the organizational culture of the foreign ministries, the main question is related to the way in which diplomats perceive digital technologies in their work: as threats or as opportunities (Bjola 2017)? Technology confronts us with many question marks because every technological innovation can be translated into the most diverse applications. If 3G technology has facilitated the spread of social networks, no one can imagine today how 5G technology could impact the socio-economic environment - answers could include existing technologies such as virtual reality, augmented reality, artificial intelligence (Sandre 2016), but whose evolution is difficult to predict. Spectacular changes have already taken place in many areas – even Romania was involved in 2016 in a disaster response exercise using virtual reality. Once the infrastructure is in place to support the optimal operation of these technologies, applications will not be long in coming, and the field of diplomacy, due to its specificity, cannot be exempted from the roller coaster of changes. If visa issuance, consular registrations or embassy assistance today are assisted by chat bots (Cresci 2017), the future may offer more sophisticated artificial intelligence algorithms capable of identifying or spreading fake news, deep fake or other forms of propaganda and misinformation (Cocking 2016).

How prepared are the foreign ministries and diplomacy to take over and capitalize on these new technologies with maximum efficiency? In order to respond, they should make an internal assessment of the degree of connection with today level of knowledge, identify ways in which technology could help achieving goals and build strategies whose application lead to the optimal implementation of innovations, including through the specialization of human resources.

1.2. Diplomacy as a reactive or anticipatory process

We have argued that the implementation of innovations an accelerated pace is strongly dependent on the human resources involved in the process. Without a suitable cognitive endowment both in terms of skills and knowledge, it is unlikely that the activity will translate from a reactive to an anticipatory paradigm. Diplomats are no longer in a position to wait for events to react for them to react also, but they have to imagine their probable scenarios and find ways to influence them.

In Romania, diplomacy seems to have become aware of the situation and is trying to outline the first steps: foreign affairs ministry is increasingly using social networks to communicate in critical situations or with the diaspora. But the stake of this period is who will become the first to be notified, in the digital environment, because that will be the one who will be able to produce the most influence.

Intelligence Advanced Research Projects Activity (IARPA) sponsored the Embers project, which by extracting data from open sources, social networks, satellite images and blogs managed to identify with a good accuracy realistic scenarios of future civil unrest, outbreaks of epidemics, political crises (Embers 2016). Through a proactive attitude, states could be open to this type of approach and could, in turn, implement such tools in their diplomatic activity.

It is expected that sooner or later Big Data tools will become mandatory for use by all foreign ministries and embassies, because no country will afford to lose the valuable information they gain. The field is going to be standardized and regulated by its pioneers, therefore the early awareness and the taking of the necessary measures in this direction will increase both the competitiveness of the diplomacy and of the country as a whole.

1.3. Degree of centralization in diplomacy: network or network of networks

In order to adapt more effectively to technological challenges, the foreign affairs ministries should relax the constraints of institutional centralization by ceding the autonomy of regional entities, thus making it possible to set up a national digital diplomatic system. Of course, everyone is subordinated to the foreign policy objectives of the states, but the diplomatic profile of the country could become systemic by including several types of actors, such as embassies, consulates, private companies, civil society (Hocking, Melissen, Riordan, Sharp 2012).

In order to adapt more effectively to technological challenges, the foreign affairs ministries should relax the constraints of institutional centralization and encourage forms and ways of digital interaction. From this perspective, the privileged role of the MFA should change and the institution should be placed in a broader structure – that of a so-called national digital diplomatic system – which it should further direct, while ceding autonomy to regional entities. Of course, everyone is subordinated to the foreign policy objectives of the states, but the diplomatic profile of the country could become systemic by including several types of actors, such as embassies, consulates, private companies, civil society.

The most important dimensions of such a system should be:

– Connecting those who need diplomatic assistance with those who have responsibilities in this field and can be assisted by digital tools (e.g. diaspora, embassies in conflict zones);

– Collaboration between the actors involved for exploring and implementing the functionalities of digital technologies in different contexts;

– Promoting innovation and disseminating good practices in digital diplomacy among system actors.

The intersection of these dimensions would require the permanent optimization of the field of digital diplomacy and would generate that impulse of creativity that allows the achievement of the proposed objectives in optimal conditions.

2. Digital Diplomacy in the European Union

2.1. Perceptions biases of digital diplomacy in the EU

We have previously shown that digital diplomacy is in its implementation phase with areas of competence transgressing from the simple communication of messages from foreign

ministries to the effective promotion of foreign policy objectives through strategies specific to current technological developments.

But the process of implementing digital diplomacy is full of obstacles, often the interpretation of the concept being erroneously made by states. According to Corneliu Bjola (2018), a common mistake is Superman Myth, which refers to the fact that digital technologies are associated with extraordinary advantages for those who use them; in the case of digital diplomacy, the use of these technologies can help increase diplomatic influence to levels that might not otherwise be achieved.

In order to have these advantages, states such as Sweden, the Netherlands, Mexico, Israel or Australia were among the pioneers of the process of digitizing diplomacy.

The misperception of diplomacy, called *the Walk in the Park Myth*, refers to the impression that the adoption of digital diplomacy is easy and inexpensive – one argument is that ordinary citizens have made the transition to digital, so it should be the same inexpensive for the states. However, the adoption of digital tools without a general strategy of how they should be used can create difficulties for foreign ministries in trying to build their digital profile and maximize the impact of their online presence. Therefore, it is necessary to invest in infrastructure, training and professionalization of staff, by developing skills with which they can strategically capitalize on the power of digital platforms in order to achieve predefined and measurable objectives.

The third misperception is Extinction Myth, according to which digital diplomacy will gradually replace all traditional forms of diplomacy. Moreover, that digital technologies have the ability to fundamentally change the way diplomats perform their traditional functions of representation, communication and negotiation to the point where diplomacy even end and is replaced with virtual embassies using virtual reality (VR) and artificial intelligence (AI) technologies.

However, although digital technologies are revolutionizing the way diplomats operate, the essence of diplomacy (i.e. building and managing relationships) cannot be achieved without human contact. The number of diplomats can be reduced, part of their activity can be taken over by machines, but the human relationship is never feasible to be replaced.

Darth Vader Myth is another bias that promotes the idea that the positive potential of digital platforms is always hijacked for dark and hidden purposes, for propaganda use. Of course, regulating the digital environment and setting certain standards can eliminate or significantly reduce the occurrence of such situations.

As information and communication technology advances, people will continue to be even more connected, perhaps in different ways than they are today. That is why it is important for digital diplomacy to accept the risks and assume them in order to benefit from the related advantages.

2.2. Good practices in digital diplomacy in EU countries

The COVID pandemic has been a catalyst for the widespread use of digital technologies. Everyday face-to-face events have been replaced by platforms such as Zoom, Meet, Teams, Moodle, online commerce has become much more used, all of which being driving factors to increase digital interdependence. Data, artificial intelligence, fake news, social media are increasingly present topics in discussions between international actors.

For example, the French strategy adopts a paradigm of openness for an inclusive internet governance, promoting the need to take measures to increase confidence in the online environment (https://www.diplomatie.gouv.fr). From his point of view, the European digital model should reflect a strengthened balance between the perspectives of states and stakeholders with different backgrounds, even nominating a technical ambassador who has the task of transforming France into an important digital hub (Kurbalija 2021).

In the Dutch strategy, the term digital security includes cyber security, human rights and the use of data, in terms of privacy, personal data protection, identity protection (Kurbalija 2021).

3. Digital Diplomacy in Romania

The need to digitize Romanian diplomacy is evident in the statements of officials, such as Foreign Minister Bogdan Aurescu, who stated that "between September 7-9, 2020, we organized, for the first time in digital format, the Annual Meeting of Romanian Diplomacy, on the impact of the pandemic". It was a real exercise in digital diplomacy - thus, the digitization of the most extensive, but also the most delicate analytical conversation of the MFA was, in itself, a conceptual and technical test" (Aurescu 2020).

Earlier, on July 1, 2020, during an international video conference dedicated to the digital response to the COVID-19 pandemic, he also stated that "the pandemic (Covid-19) has interrupted many processes, but certainly accelerated the digitization, which is a priority for the EU, including for the Government of Romania" (Aurescu 2020). From his point of view, the diversification of digital services and the education of specialized skills for human resources are priorities of Romania in this period. The Final Declaration of this videoconference, attended by foreign or communications ministers from 60 countries on five continents, states the "rapid consolidation of digital capabilities in health systems, ensuring a safer digital space, building modern healthcare systems. e-government, providing affordable connection in any area of the globe, protecting human rights and fundamental freedoms, freedom of the internet, stimulating online commerce, improving digital skills and literacy, and reorienting financial resources to support transformation digital" (Aurescu 2020).

These positions represent clear evidences that digitalization is a priority for the relevant ministry of our country, included in the Romanian government program for 2020-2024. National objectives are conceptualized in accordance with the Digital Package adopted by the European Commission on 19 February 2020 (Communication on Configuring Europe's Digital Future, the European Data Strategy and the White Paper on Artificial Intelligence). The first step was taken in 2001, when the first website of the Ministry of Foreign Affairs was built, followed by the subsequent relatively intense use of social networks.

Despite the explicit intention to digitize diplomacy, Romania does not have a clear strategy that provides both an overview and clear ways to follow to achieve these goals.

However, in order to achieve these goals, it is necessary for the foreign affairs ministry to adopt a digitization strategy that will require in particular:

- an explicit, unambiguous vision of digitization
- unequivocal assumption by decision-makers of the digitization process
- training of human resources in the field of technologies, emphasizing the benefits and risks
- identification and popularization of good practices in the field
- designing training programs dedicated to the training of digital skills of diplomatic staff.

We consider that each aspect mentioned above is important, although the key dimension is related to human resources. Foreign affairs ministry' institutions such as the Romanian Diplomatic Institute, but also other training organizations in the field (SNSPA, University of Bucharest, "Carol I" National Defense University, National Institute for Research and Development in Informatics, European Security and Defense College of the EU) can be involved for achieving this goal. For example, the European Security and Defense College of the European Union has already developed a series of profile courses in collaboration with

institutions of European countries, including ICI Bucharest and can provide expertise to achieve the best results.

Conclusions

Once we understand the impact that technology has on international actors, we can identify possible behaviors and resources that are more likely to provide a stronger or weaker influence on the evolution of the international system. Each crisis is unique in its own way, and digital diplomacy will contribute to a better understanding of it through the knowledge produced regarding the various variables that led to its onset: the nature, stage, dynamics and location of the crisis, possible paths of evolution. These variables can be assessed through diplomatic analysis, including through the use of the benefits of digital technologies, which collect, process and report information to the competent decision-making and crisis management bodies.

We have previously shown that digital technologies need to be first understood and only then implemented in order to achieve the efficiency of the process. Also a few directions of action should be considered:

1. Measures that lead to the overlapping of the public perception with the foreign affairs ministry's self-image, in order to eliminate the errors of public perception towards the foreign policy of our country;

2. Measures to implement an infrastructure capable of supporting the activities subject to digital diplomacy and related online networks;

3. Measures dedicated to the training of the competencies necessary to carry out digital diplomacy activities for the human resource in the diplomatic corps.

The field of digital diplomacy is insufficiently implemented in Romania, but we have shown that achieving Romania's competitiveness is impossible if not all available methods are used to achieve national objectives. Therefore, decision makers are in a position to make fundamental modernization options that can strongly impact the future of Romania and its citizens.

Acknowledgement
This paper is published within the doctoral program Intelligence and National Security of "Carol I" National Defence University.

BIBLIOGRAPHY:

BJOLA, C. 2017. "Adapting Diplomacy to the Digital Age: Managing the Organisational Culture of Ministries of Foreign Affairs", Working Paper, Project - Diplomacy in the 21st Century (Berlin Stiftung Wissenschaft und Politik), URL: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_Diplomacy21_No9_Corneliu_Bjola_01.pdf

BJOLA, C. 2018. "Digital diplomacy – from tactics to strategy". The Berlin Journal no. 32. URL: https://www.americanacademy.de/wp-content/uploads/2018/09/20180926_Berlin-Journal-32-Fall-2018.pdf

CHAKRABORTY, K. 2013. *Cultural Diplomacy Dictionary*, Berlin: Academy for Cultural Diplomacy, URL: http://www.culturaldiplomacy.org/culturaldiplomacynews/content/pdf/Cultural_Diplomacy_Dictionary.pdf

COCKING, S. 19 September 2016. "Using Algorithms to Achieve Digital Diplomacy", Irish Tech News. URL: http://irishtechnews.ie/using-algorithms-to-achieve-digital-diplomacy-a-conversation-with-elad-ratson-director-of-rd-at-ministry-of-foreign-affairs/

CULL, N. J. 2008. "Public diplomacy: Taxonomies and histories", in The Annals of the American Academy of Political and Social Science 616.

Digital Watch. URL: https://dig.watch/issues

DREISCHMEIER, R.; CLOSE, K. and TRICHET, P.. 2 March 2015. "The Digital Imperative". The Boston Consulting Group. URL: https://www.bcg.com/en-hu/publications/2015/digital-imperative

European Commission. 2021. "Digital Economy and Society Index (DESI) 2020", URL: https://digital-strategy.ec.europa.eu/en/policies/desi.

HOCKING, B.; MELISSEN, J.; RIORDAN, S. and SHARP, P. 2012. "Futures for Diplomacy: Integrative Diplomacy for the 21st Century", The Hague: Netherlands Institute of International Relations 'Clingendael'. URL: https://www.clingendael.org/sites/default/files/pdfs/20121030_research_melissen.pdf

KURBALIJA, J. 2021. "The emergence of digital foreign policy", URL: https://www.diplomacy.edu/blog/2021-emergence-digital-foreign-policy

MAE . 2020. "Diplomația română în 2020: Testul crizei pandemice și dincolo de aceasta", interview of Foreign Affairs Minister Bogdan Aurescu to Digi24, 09.09.2020, URL: https://www.mae.ro/node/53600

MAE . 2020. "Participarea ministrului afacerilor externe Bogdan Aurescu la Conferința internațională dedicată răspunsului digital la pandemia COVID-19", URL: https://www.mae.ro/node/53008

Media Hotnews. 2020. "Program de guvernare 2020-2024", URL: https://media.hotnews.ro/media_server1/document-2020-12-23-24501757-0-program-guvernare-citu.pd

PERDUE, T. 20 Iune 2018. "Applications of Augmented Reality", Lifewire, URL: https://www.lifewire.com/applications-of-augmented-reality-2495561

SANDRE, A. 2016. "Virtual Reality for Digital Diplomacy", Digital Diplomacy. URL: https://medium.com/digital-diplomacy/2016-in-review-virtual-reality-for-digital-diplomacy-b461ac2ff16

Swiss Federal Department of Foreign Affairs FDFA. 2020. Digital Foreign Policy Strategy 2021-2024. URL: https://www.eda.admin.ch/dam/eda/en/documents/publications/Schweizerische Aussenpolitik/20201104-strategie-digitalaussenpolitik_EN.pdf

WEINER, T. 26 June 1996. "Citing Security Threat, Maps a War Plan on Hackers", International Herald Tribune.

DOI: 10.53477/2668-6511-22-16

SECURITY DYNAMIC OF THE STRATEGIC NUCLEAR BALANCE IN SYSTEMS THEORY AND THE CONCEPT OF CENTRES OF GRAVITY

Mario MARINOV,
Ph.D. Candidate, University of Library Studies and Information Technologies,
Sofia, Bulgaria.
E-mail: m.marinov@unibit.bg

Plamen BOGDANOV, Ph.D.,
Brig.-Gen. (ret.), Associated Professor,
University of Library Studies and Information Technologies, Sofia, Bulgaria.
E-mail: p.bogdanov@unibit.bg

Abstract: *The general concepts and understandings of the international security environment in the 21st century have become more complex owing to a multitude of factors spanning both traditional and novel security domains. In the current era, nuclear security in particular has continued to exist in its paramount role of importance. The following paper explores the defined state of the "strategic nuclear balance" as a state extant within the systemic approach towards international security. Based upon previous research in defining the state through core concepts fundamental to systems theory and supporting concepts such as those of centres of gravity, this paper aims to further expand contemporary understandings and illustrate a point of coalescence. Thereby the given study demonstrates how based upon key postulations in the understanding of the security concept in systems theory and centres of gravity of both physical and non-physical nature within a system, a combined novel model can be extrapolated, which demonstrates the security dynamic in the "strategic nuclear balance" between major global nuclear armed state actors.*

Keywords: *strategic nuclear balance; centres of gravity; systems theory.*

Introduction

The complex international security environment of the 21st century offers a diverse and ever-expanding array of challenges in maintaining peace and stability, ranging from the traditional domains of warfare and the novel threats that have come to permeate them to the technologically revolutionary new domains of space and the digital realm. The theoretical application of models is vital in establishing a coherent dynamic that can explain past, present and emerging security phenomenon, as well as in anticipating their effects. Amongst the challenges to security, stability and peace, and a subject area of particular and continuing interest for all major global actors, is the nuclear security sphere, whose continued importance has not dwindled since its apogee during the latter half of the Cold War, and which now stands once again as the preeminent factor of importance in shaping the strategic landscape of tomorrow. In providing for future stability the subject matter of nuclear security, necessitates continued discussion and theoretical analysis encompassing the examination and superposition of past such efforts with contemporary ones.

The following paper serves the primary purpose of further expanding previous research into the theoretical understanding of the *"strategic nuclear balance"* in systems theory and the notions therein of *"security"* as a fundamental state of a system, where the *"strategic nuclear balance"* has previously been defined as *the extant moment security state derived in the international system of relations from the security interactions of the constituent sub-systemic elements* of the national subsystems. These national subsystems in the international system are considered to be foremost global nuclear powers, which possess the highest degree of potential to precipitate change in the international system, and are themselves viewed as complex recursive systems possessing other complex systems within them, and which through their own interactions and structure coalesce into the operations and capabilities of the larger national subsystem. The paper further expands upon previous efforts in collaborating the security environment dynamic in the *"strategic nuclear balance"* through the implementation of the concept of *Centres of Gravity* (*CoGs*), as fundamental in understanding the security state on both the highest order systemic level of the international system, and the recursive national subsystem levels within it.

Thusly, the following paper has as its ***main object of theoretical analysis*** the *"strategic nuclear balance"*, with the ***principal subject*** being *the further implementation and coalescence of systems theory and the concepts of Centres of Gravity in a more precise and clearer model, showcasing key dependencies and set dynamic*.

The ***working thesis*** of the paper is that *based upon the key elements of zones and levels of security in the systems-based approach towards international relations, as well as the concept of centre of gravity, a model of the evolution of the "strategic nuclear balance", which this paper has dubbed the "Hourglass Model", can be established. This model showcases the dynamic between levels of security and Centres of Gravity of two national subsystems, the dynamic of their transition within the international systems and within different zones of security, creating points of balance, or points of great disbalance, where security risks and threats are at their highest values*.

In its structure the paper will adhere to the following ***methodology***:

– The paper will first examine the notion of *"security"* as a dynamic state based on systems theory, utilising the additional notions of levels and zones of security as key components in understanding its exact dynamic across the systemic levels of the *"strategic nuclear balance"*;

– The paper will then reiterate the key points of *CoGs* within the individual systemic levels of the *"strategic nuclear balance"*, as well as their expression;

– Finally, the paper will seek to establish a model of interactions between *CoGs* and *levels and zones of security*, demonstrating their mutual dependencies and overall dynamic.

In exploring the notions of the *"strategic nuclear balance"* the paper will adhere to several ***limitations*** for the purposes of narrowing down its ***scope***. Within systems theory and the exploration of the concept of *"security"* as an element within the international system, the following paper will not focus on the individual examination of the concept within specific national subsystems, where perceptions and definitions of *"security"* inevitably vary, but will instead focus on *"security"* as a state or condition of the system/s based upon the key requirements for overall existence, regardless of the examined national security system. Furthermore, the examination of the *"strategic nuclear balance"* within this approach will primarily focus on the dynamic between the highest order systemic level of the international system and the constituent lower order systemic levels of the national subsystems. These specific interactions are considered to be of the highest value in establishing a dynamic within the *"strategic nuclear balance"*. The national subsystems, when examined through systems theory are in their own right complex recursive systems possessing other lower order systems,

which make up their structure and operation, offering additional avenues of exploration in further defining systemic behaviours, but are outside the scope of the present paper. Additionally, when examining the *"strategic nuclear balance"*, which traditionally entails the exploration of the specific historical nuclear-superpowers and their specific security concerns within the international system, the following paper will instead focus on providing the theoretical basis for a model of the dynamic within the *"strategic nuclear balance"*, where the constituent nuclear superpowers will simply be referred as Subsystem A and Subsystem B, or overall the national subsystems within the international system. Finally, for the purposes of this paper, an in reiteration of the previously stated chosen approaches towards the analysis of the *"strategic nuclear balance"*, it is defined as *"a dynamic state with moment values within a given time interval and within the framework of a complex system of interactions. This complex system of interactions is at its highest order the "international system", and is constituted by interacting recursive hierarchical complex subsystems, with the primary such subsystems and the ones most vital in forming the "strategic nuclear balance" being the national subsystems."*

1. Levels and Zones of Security in Systems Theory and the "Strategic Nuclear Balance"

In understanding the *"strategic nuclear balance"* through the lens of systems theory, of paramount importance are the concepts of *"security"* and the *"security state"*, as the particular condition in terms of security perceptions of a system at any specific time. However, *"security"* is an ambiguous concept with widely varying definitions and perceptions across specific nations, languages, cultures and historical periods, as examined within the complementary organisations-based approach towards understanding the behaviour of systems. The task of its precise understanding, definition, and implementation is a daunting challenge, and requires an individualistic approach towards its exploration in each individual national subsystem level, and thus falls outside of the scope of the current paper. Instead of attempting to provide such a definition of *"security"* for each systemic level, which will inevitably vary in its precise content, within systems theory and specifically the operation and dynamic of a security system, the following paper will employ the terminology established by E. Manev for the set of primary elements employed in constructing the *"security"* concept and the same such elements necessary for its continued function (Manev et al, 2017, 33-34):

– ***Security levels*** *– moment values indicating the probability of unwanted events occurring, which have the high probability of decreasing the nominal functioning of the system.*

– ***Security zones*** *– intervals, within which the security levels correspond to set requirements and within which the security level can vary between given boundaries.*

– ***Normal state*** *– the state when a system can function under its established organisational, architectural and functional model;*

– ***Nominal state*** *– the state when a system functions closest to its predicted optimal state, thereby possessing the maximum possible security level.*

– The security dynamic is further expanded in the specific characteristics of the three defined zones of operations for a given system and its subordinated subsystems (Manev 2016, 265):

– ***Normal security zone*** – where the system operates within its defined nominal state and parameters of operations, and where the security level can deviate in expected and manageable margins, close to the optimal state, as such in this zone the system is guaranteed the highest level of security and there are no apparent risks for its structural integrity.

– ***Emergency security zone*** – where the system, due to the emergence of factors has passed outside of the normal zone of operations, and therefore experiences heightened risks and

threats to its integrity, thus producing a lowered security level. In this zone the systems undertake planned steps to return to the normal zone of operations.

– ***Catastrophic security zone*** – where the system's integrity and operations have been degraded to the extent where operations are no longer possible and there are insufficient resources within it to restructure itself and return to the normal zone. In this zone the system can no longer provide for the levels of security for continued existence. Past this zone the system faces either complete collapse, or complete restructuring through outside intervention and input of resources.

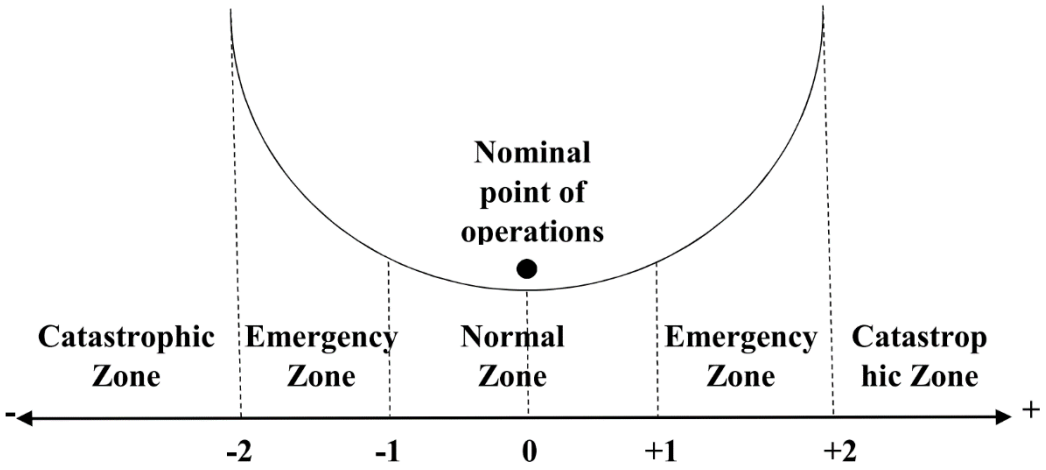

Figure no. 1: Zones and Levels of Security (Manev et.al. 2017, 35)

When the system transitions from one zone to the other it follows the dynamic of moving from one security level to the other (as numerically abbreviated in the below graphic [Fig.1]), potentially progressively moving from the highest security level, where there is a lack of direct threats or risks, towards a lower security level (the lowest being the catastrophic zone where the system is overwhelmed), or rebounding to again return to a higher security level (Manev et al 2017, 34).

In the international system and the systems-based approach towards understanding the *"strategic nuclear balance"*, the *"normal zone"* and *"normal state"* of operations can be considered to revolve around the primary systemic objective of structural survival of any given system. In the *"normal zone"* and within the notion of the *"strategic nuclear balance"* such a *normal state* of ensured survival can be constructed around the concept of *"deterrence"* where all constituent national subsystems must find themselves in a state of equally perceived levels of deterrence and equally accepted notions of *"mutually assured destruction"* (Marinov 2020 (1), 770-773). When such conditions exist, both the international system and the national subsystems can be stated to have achieved a nominal state and level of security, as the threats of destabilisation and collapse at all systemic levels are at their lowest values. Such a state has historically been further defined in specific qualitative and quantitative values in nuclear arms striving towards mutually acknowledged parity, and has been the desired state for the nuclear super-powers in previous decades (Marinov 2020 (2), 66-67).

Additionally, the following additional notions must be taken into account in the specifics of the *"strategic nuclear balance"*, when precipitating change in systemic levels, namely (Marinov 2020 (2), 66-67):

– The nominal and optimal levels of security in the highest order system – the international system, are subject to the actions and interactions between the national

subsystems. Therefore, the actions of one subsystem can unliterary and significantly alter the overall state of the international system and its levels of security.

– Any given national subsystem can proceed to have a defined *"optimal security level"* that is drastically different from the moment values of the security level in the international system. When such an occurrence takes place there are immediate consequences for both the levels of security in the international system, and the corresponding other national subsystems, which will also strive to change their respective security levels to ensure a return to the *"normal zone"* for their respective operations, thus continuing and propagating the effects of change and transition in the zones of security in the international system, pushing the higher order system towards either further destabilization or coalescence around a new "normal state" of operations for all systems [Fig. 2]. Such a dynamic can be stated to also correspond in part to the concept of the "security dilemma" in the realist school of examining international relations, where various extrapolations of state behaviour and eventual conflict evolution have also centred on the notions of mutual fear. However, a clear distinguishing characteristic of the approach proposed here is that it offers a more holistic method towards defining an overall dynamic and specifically the necessary context for establishing rules and preconditions for conflict prevention in the nuclear era. In conjunction with the organisational approach, such an approach towards nuclear security in particular are the individualised and specific extrapolations of national subsystem behaviour based upon their specific organisational characteristics and security perceptions.

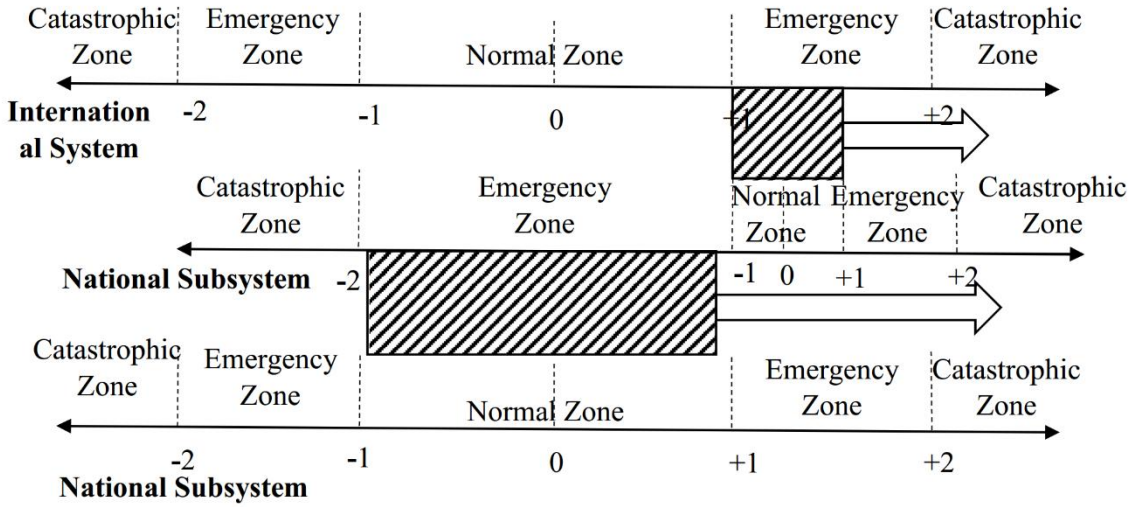

Figure no. 2: Levels and Zones of Security in Systemic relation
in the "Strategic Nuclear Balance" (Marinov. 2020 (2), 66)

2. Centres of Gravity in the Strategic Nuclear Balance

Centres of Gravity stand as the next vital concept in constructing a coherent model for the security dynamic of the *"strategic nuclear balance"*. *CoGs* in their own right have been a vital notion in projecting and understanding the balance of military power between adversaries, ever since Clausewitz first established the concept in the 19th century. The concept, its precise definition and implementation in modern military strategy, remains a topic of heated discussion to this day. *CoGs* have been postulated to possess both physical and non-physical characteristics, pertaining both to one's own capabilities and those of adversary, and constituting the elements, which when neutralised would either significantly reduce military capabilities and or possess the ability to achieve victory in tactical, operational and strategic terms, as per M. Vego's definition: *„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" (Vego 2017, 43).

CoGs also have systemic characteristics, where the degradation of the systemic connections and the stability of a given system would be rendered inoperable the adversary's or one's own military capabilities, as per A. Echevarria: *„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"* (Echevarria 2002, 16).

Both concurrent definitions are applicable in understanding the security dynamic of the *"strategic nuclear balance"* albeit at different systemic levels and in consideration of the specific characteristics of these levels.

On the national subsystem level, *CoGs* constitute the physical elements of strategic nuclear power. However, unlike traditional *CoGs*, which manifest in a conflict and whose effectiveness is intrinsically tied with effectively destroying the adversary's *CoG*, whilst protecting one's own, in the *"strategic nuclear balance"*, the inherent vulnerability to the far-reaching structure of two complex national subsystems afforded by strategic nuclear arms is the ultimate instrument in ensuring their individual survival through the concept of *deterrence*. The greater the disparity in capabilities between the two subsystems, the greater the associated threat level that will be perceived by the one side. Consequently, and in the interest of mitigating security concerns on the level of the international system, national subsystems have historically moved towards strictly defining their individual *CoGs*, creating an environment of mutual predictability, and placing limitations and values on their qualitative and quantitative characteristics, creating the idea of nuclear parity, as a quintessential element of strategic nuclear stability and consequently the *"strategic nuclear balance"*. Such processes and the very concept of negotiating power distribution and parity through a treaty system are not confined to the history of the *"strategic nuclear balance"* and modern international relations, but are the historical result and principal method of operation and interaction of social organisations in general, which the national subsystems examined can be defined to be. The phenomenon has been prevalent in previous historical periods – the Washington and London Naval Treaties sought to achieve such results in the international system in qualitative and quantitative terms for capital ships, which were considered the mechanism for strategic power projection of that era; the preceding era of the "Bismarck system" sought to produce contrasting alliances of equal power level in balancing European powers and their global ambitions; even in the historical record of treaties between the Roman and Persian Empires, the idea of territory distribution in the border-regions of the two empires is centred around parity in spheres of influence. In the nuclear era the major global nuclear super-powers utilise the instrument of the bilateral treaty obligations and specific limitations to establish a working *"nuclear treaty regime"* again centred on the idea of parity. This "regime" or framework of treaties, as well as the associated levels of mutual trust that form in their continued existence and application, establish the basis for the non-physical *CoG* in the international systemic level that comes to dominate the *"strategic nuclear balance"* and govern its dynamic (Marinov (3) 2020, 309-310).

When in such a framework of relations, one subsystem moves to change the exact characteristics of its physical *CoGs* owing to a variety of factors, it establishes the preconditions to immediately degrade this non-physical *CoG* and precipitate equal reaction from the other subsystem. Consequently, the disparity in capabilities drastically increases past this point, and

the proportionally increases the respective security concerns and consequences for the *"strategic nuclear balance"*.

3. The "Hourglass" Model and the Security Dynamic in the Strategic Nuclear Balance

Having first explored the concept of *"security"* through the lens of systems theory and specifically the application of levels and zones of security in extrapolating a security dynamic in the *"strategic nuclear balance"*, as well as having examined the concept of *"Centres of Gravity"* and its application across systemic levels, the next logical step is to form the basis of a model that combines the efforts thus far in establishing a coherent picture of the security dynamic of the *"strategic nuclear balance"* across time, and which will serve as a baseline model for further studies, as well as potential additions and revisions.

The proposed model is demonstrated in the graphic below, which has been named the "Hourglass Model" [Fig. 3] and will be explained further in this section of the paper:

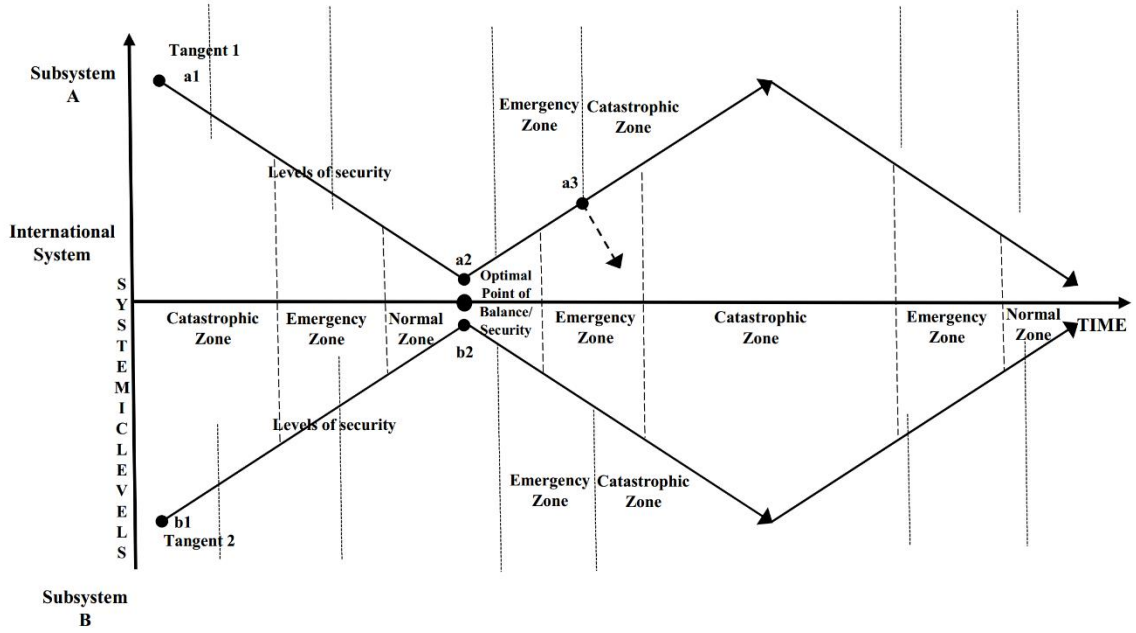

Figure no. 3: *"Hourglass Model"* of Zones and Levels of Security, and Centres of Gravity Interaction in Forming the *"Strategic Nuclear Balance"*

At its very essence the presented "Hourglass Model" is spread across two axes ***"Time"*** and ***"Systemic levels"***, where the horizontal axis demonstrates the flow of time, and vertical axis encompasses the systemic levels, examined as key to the *"strategic nuclear balance"*, these being namely the highest level of the ***"International System"*** and the subsystem levels, or national subsystems, of the global major nuclear powers listed as ***"Subsystem A"*** and ***"Subsystem B"***. On the graphic of the model, ***Subsystem A*** is depicted above ***Tangent 1***, ***Subsystem B*** depicted below ***Tangent 2***, and the ***International System*** is depicted between ***Tangent 1*** and ***2***, or "inside" the hourglass structure.

Across these levels of the system and across time a certain dynamic develops, which encompasses several key values of the variables spread across the graphic, and are namely:

– ***Tangents 1*** and ***2***, which form the proverbial "walls" of the hourglass and encompass both the relative levels of balance between the *CoGs* of the two Subsystems, as well as marking the dynamic in levels of security and the exact span of security zones across systemic levels.

– ***Points a1***, ***a2***, ***b1***, ***b2***, ***c1***, which mark specific points in the balance between *CoGs*, as well as specific points in the levels of security shared across all systemic components.

At ***Points a1*** and ***b1***, the relative disparity in capabilities between the *CoGs* of both Subsystems (representing, as previously stated for the national subsystems, their physical strategic nuclear power) is at its highest levels. It is also at these points that the levels of security are at their lowest values for both the subsystems, as well as for the higher order international system, and all exist in the ***"catastrophic zone"***, where the risk of a conflict breaking out is at its highest.

Subsequently and in order to increase relative levels of security in the international system and to ensure their own survival, both subsystems move to bridge the gap, aligning their security perceptions articulated in equally expressed zones of security, and advancing along both ***Tangents 1*** and ***2***, towards ***points a2*** and ***b2***, respectively. In this dynamic the relative disbalances in *CoGs* are gradually eliminated, which in the *"strategic nuclear balance"* is seen as the establishment of a clear and mutually acknowledged state of necessary *"deterrence"*. In historical terms, this has implied the gradual reduction of nuclear arsenals to more manageable and equal levels, elimination of weapons classes that can be detrimental to the security perceptions of both sides, the establishment of clear channels of communications in emergency scenarios, and most importantly the extension of all such efforts through the established toolset of the international system, materialising in a framework of regulatory mutual treaties, the so called *"nuclear treaty regime"*.

This dynamic has its apogee at ***points a2*** and ***b2***, where the strategic nuclear power (both offensive and defensive) of both subsystems is near equal. It is also at this point that both the international system and its subsystems in their levels of security have reached a mutual ***optimal point of security perceptions*** and where the definition of an existent and true to the word *"strategic nuclear balance"* can exist. Within this ***"normal zone"*** of operations for the international system, the primary goals of assuring peace and stability, and therefore a near lack of security risks and threats, are achieved and maintained. The treaty regime at this point in the security dynamic, stands as the non-physical *CoG* of the international system and thus its degradation will move the overall system again towards lower levels of security and greater disbalance.

Whilst a continued state of affairs, such as the one existing within the ***"normal zone"*** of operations for all systemic elements is preferred and desirable, it cannot be maintained in perpetuity. The even larger international security system and the organisational characteristics of national subsystems as social organisations and complex systems in their own right are extremely dynamic, and a change in overall security policy or an increased perceived threat in one subsystem from the other, results in that subsystem's security perceptions and corresponding levels of security changing values. Such a perceived threat could also come from other subsystems in the international system, which over time could have advanced the capabilities to constitute a new factor in the ***"strategic nuclear balance"*** and its dynamic. Consequently, a ***Subsystem*** in such conditions would seek to expand its direct nuclear capabilities, changing the characteristics of its *CoG*, and diverging from the ***optimal point of balance*** with the other principal ***Subsystem***, thus precipitating equal requirements for change within it. However, such a change in the physical *CoGs* of both ***Subsystems*** would entail a degradation of the non-physical *CoG* of the international system, the *"nuclear treaty regime"*, which seeks to govern ***Subsystem*** **CoGs**, pushing the international system towards the emergency zone, and finally into the catastrophic zone.

In this latter half of the dynamic, and particularly in the ***"emergency zone"***, a Subsystem could undertake steps, as in ***Point a3*** to return to a point of balance, thus serving as the basis for the potential emergence of a new "normal zone". However, in an environment permeated by a lack of mutual efforts, or in the case of the emergence of a new significant subsystem (a new major strategic nuclear power), as well as a subsystem unwilling to effectively engage with its peers, the outcome is a clear transition to the ***"catastrophic zone"*** and the collapse and subsequent reconstruction of the international system through significant global geopolitical changes.

Conclusion

This final process in the demonstrated model of the security dynamic of the "strategic nuclear balance" has in the past constituted significant historical outcomes in the international security system – the established system of the international power balance (the "Alliance system") prior to 1914 and its inability to overcome a moment of crisis resulted in World War I; the subsequent system of the League of Nations, and its constituent Washington and London Naval Treaty regimes could not in the end overcome significant systemic challenges to preserving international peace and preventing an arms race, resulting in their collapse. The consequences for the *"strategic nuclear balance"* from a general transition to the catastrophic zone are far more severe. Uniquely and conversely to the above episodes within the international system, the gravity of nuclear weapons and the outcomes of their perspective employment have historically transitioned the system through variable points of emergency in the past seven decades. Within the proposed model, of interest are the effects of introducing a third significant national subsystem, making the observed model from a two-dimensional one to a three-dimensional one. The effects of continued technological progress, the further militarisation of space and the development of both novel offensive and defensive strategic weapons systems, are also vital in further extrapolating the future dynamic of the *"strategic nuclear balance"* and the direct effects to subsystem *CoGs* and security perceptions. The behaviour of the specific national subsystems in the international system also depends of numerous specific and unique organisational characteristics pertaining to the very essence of the security concept. All of the above; however, fall outside of the scope of this paper, and would serve as the basis for the future expansion and refinement of the proposed "Hourglass" model, which has thus far combined key approaches in understanding the security dynamic in the international system through systems theory, the specifics of the "strategic nuclear balance" within it, as well as the associated Centres of Gravity that develop and evolve around the main systemic elements.

BIBLIOGRAPHY:

***, Глобална, регионална и национална сигурност [author's translation: *Global, Regional and National Security*]

***, Определение за сигурост – организационнокурурен подход [author's translation: *Definition of Security – an Organizational-Cultural Approach*]

***, Системен подход за анализирането на съвременния стратегически ядрен баланс като елемент на международната система [author's translation: *Systemic Approach for Analyzing the Contemporary Strategic Nuclear Balance as an Element of the International System*]

ECHEVARRIA, Antulio. 2002. Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine– Again!: U.S. Army War College.

MANEV, Evgeni, et al. 2016. "Определение за сигурост – организационнокурурен подход", Burgas: Journal of Legal Studies, Vol. XXIII.

MANEV, Evgeni. 2012. Глобална, регионална и национална сигурност, Sofia: Softtrade.

MARINOV, Mario. 2020. "Defining Centres of Gravity within the Strategic Nuclear Balance Between the United States of America and the Russian Federation". Bucharest: Carol I Nation Defence University.

MARINOV, Mario. 2020. "Organisational and Systems-based Approach for Defining Levels and Zones of Security within the Strategic Nuclear Balance between the United States of America and the Russian Federation". Sofia: Security – Education, Science, Industry, Georgi Rakovski Military Academy.

MARINOV, Mario. 2020. "Системен подход за анализирането на съвременния стратегически ядрен баланс като елемент на международната система". Sofia: Journal of Knowledge Society and 21st Century Humanism, University of Library Studies and Information Technologies, Sofia.

VEGO, Milan, Joint operational warfare: theory and practice, in Ion Chiocea et al. 2017. "Definitions of Center of Gravity – Evolution and Interpretations, Technologies". Bucharest: Military Applications, Simulation and Resources. "Carol I" National Defence University.

DOI: 10.53477/2668-6511-22-17

SPACE SYSTEMS – A NEW CRITICAL INFRASTRUCTURE SECTOR?

Cristian BĂHNĂREANU, Ph.D.
Senior Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania.
E-mail: cristi.bahnareanu@gmail.com

Abstract*: In recent years, space capabilities have become increasingly important for the proper function and development of the economy and society and for ensuring security. Space is the newest operating environment for military powers, so decision makers can no longer ignore the benefits of space systems and technologies, but also the risks and threats they may be subjected to. The paper highlights the the growing contribution of all these space systems to the functioning of most critical infrastructure sectors and assesses that they must be an independent sector of such infrastructures that need to be protected.*

Keywords*: space systems; critical infrastructures; national security; protection and resilience.*

In recent years, major economic and military powers have developed a major interest in the development of space systems and technologies and their use to increase the effectiveness of actions and missions in pursuing national interests. The United States, Russia and, more recently, China and the European Union, share their supremacy in space, a particularly important area in terms of applicability in civilian, commercial and military environments, especially communications, navigation, data transfer, astronomy, space exploration and monitoring, etc.

Space and space systems are vital to national security and the ability to understand emerging threats, to conduct operations and project power, to support political and diplomatic efforts, and to enable economic viability (US Department of Defense January 2011, 1). The space systems will soon become part of critical infrastructures, given the fact that they are integrated into almost all key sectors, whether we are talking about the economy and society or national security.

1. Critical infrastructure – some theoretical considerations

The concepts of *infrastructure* and *critical infrastructure* have been the subject of significant debate by decision-makers and the public, especially in United States, since the Cold War. After a long evaluation and re-evaluation process, the US Congress adopted the *USA Patriot Act of 2001* (US Congress 2001, 401), which provided a new critical infrastructures definition: "systems and assets, whether physical or virtual, so vital to a country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". The 2002 *National Strategy for Homeland Security* (US Office of Homeland Security 2002, 29-30) reaffirms the definition of critical infrastructure and sets out the reasons why certain infrastructures are classified as critical, especially because of the functions or services they provide to the country, but also because of the complexity of those systems – the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.

The 2003 *Homeland Security Presidential Directive 7 on Critical Infrastructure Identification, Prioritization, and Protection* (The White House 2003) adopts the same

definition of critical infrastructures provided by *USA Patriot Act* and the classification of critical infrastructures and key assets (13 sectors) stipulated in the 2003 *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (The White House 2003, 36-79). About 10 years later, the 2013 *Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience* (The White House 2013) extends critical infrastructures to 16 sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems. The list of critical infrastructures and key assets remains open and may be extended as risks and threats evolve.

NATO has largely adopted the US model and has paid particular attention to all identified categories of critical infrastructures, in particular to their protection against military threats. According to Allied Command Operations, critical infrastructure is a nation's „infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political, and/or social life on which a nation and/or NATO depends" (Bearse 2021, 10). These include all the vital components of security, governance, public health and safety, the economy and the level of public confidence, incapacity or destruction of which could seriously affect a country's ability to function effectively.

The European Union has also taken important steps to address critical infrastructure issue. According to the European definition, critical infrastructure include "physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments" (European Commission 2005, 20). The results of the debate on critical infrastructure protection were presented in the *European Programme for Critical Infrastructure Protection* (European Commission 2006), a framework document defining EU options to prevent terrorist attacks, cyber attacks and misinformation, force training, launch specific responses to protect Europe's critical infrastructure. The package of specific measures aims to improve the protection of critical infrastructures in Europe, in all EU Member States and in all relevant sectors of economic and social activity.

2. Space systems development

Since the first launch of intercontinental ballistic missiles and the Sputnik satellite (the 1950s), there have been concerns about the possibility of launching an arms race into outer space by the main actors – the United States and Russia. The *Outer Space Treaty* (United Nations Office for Outer Space Affair 1966), supplemented by the *Moon Agreement* (United Nations Office for Outer Space Affairs 1979), laid the groundwork for slowing down or at least limiting the pace of space militarization by banning 111 signatories from carrying nuclear or any other kinds of weapons of mass destruction in orbit around the Earth and the Moon, install such weaspons on the surface of the Moon and other celestial bodies, or station such weapons in outer space in any other manner.

At present, *space systems* encompass a number of aspects, from the ability of a space asset to accomplish a mission to the ability of terrestrial-based asset to accomplish a mission in or through space or the ability of a space asset to contribute to a mission from seabed to the space domain (Joint Chiefs of Staff 10 April 2018, GL-6). The most important space systems (Sellers 2015) that can be used both peacefully, for civil and commercial purposes, and in the military field are: communications satellites (voice communications, satellite television, broadband internet, mobile services and data transfer services); intelligence, surveillance and reconnaissance satellites (remote sensing data, including data on land, sea and Earth's atmosphere); navigation satellites (positioning, navigation and synchronization data); science

satellites, stations and probes (exploration, research and experiments); command and control architecture (how users control and communicate with satellites or terrestrial systems); space launch facilities (ability to deliver useful tasks in space); government agencies, companies and universities (advanced research and development capabilities and technological implementation), etc.

Space research seems to have booming lately, and private companies and some states have set bold goals to explore the near universe, improve terrestrial life, and increase security and resilience to space phenomena that could threaten Earth. Thus, the space sector is in a new stage of development, technological innovations and new space systems are emerging, from microsatellites to constellations of hundreds of satellites, small launchers, broadband internet and Internet-of-Things (IoT), manned commercial flights and so on. However, despite predictions in the 2000s about the progress of rockets and launch and deployment technology, change has been slow. Thus, the costs per kilogram of payload placed into orbit remained similar to those of Saturn rockets and the Apollo program (late 1960s and early 1970s). Much more progress could be made in the near future, as reusable SpaceX and Blue Sky rockets could reduce costs by approximately 50-75%. (O'Hanlon September 2018, 19).

Over the past five years, we have witnessed the rapid expansion of public services and products using satellites and related technologies, such as communications, satellite television services, or geospatial products. On September 1, 2021, the situation of operational satellites currently in orbit around Earth was as follows: US – 2.788 satellites, China – 431, Russia – 167, other countries – 1.164 (UCS Satellite Database 2021).

Table no. 1: *Number of launches and satellites in 2021* (UCS Satellite Database 2021) (Kyle 2021)

	US	**China**	**Russia**	**India**	**UK**	**Germany**	**France**
No. of orbital launches	43	55	25	2	-	6 (Europe)	
No. of satellites	2.788	431	167	61	347	47	31

A newer trend is the use of microsatellites, especially in commercial and civil areas, in the area of Earth observation, remote communications and weather forecasting. Armed forces could use this technology to create more resilient and less vulnerable communications networks to anti-satellite weapons or to continuously track larger ground objects, such as intercontinental ballistic missiles. The Russian test of a direct-ascent anti-satellite weapon, destroying one of its own low-earth orbit space objects, a defunct satellite (Raju 2021), demonstrates the very real threat to space systems.

It is true that space power refers to the means of deterring, defeating, destroying and, in some cases, denying access to space for military or civilian purposes to potential adversaries, and space systems provide critical combat capabilities with the possibility of producing effects far superior to those on land, air or sea. Space is a new dimension of the modern warfare in which the great powers seek to develop new military capabilities in order to strengthen their national security. The growing importance of space for security has also led many countries to consider the need to develop their own counterspace capabilities – whether cybernetics, targeted weapons, electronic warfare, anti-satellite missiles, potentially offensive orbital systems and so on – which can be used to deceive, disrupt, deny, degrade, or destroy an adversary's space systems or services (Joint Chiefs of Staff 10 April 2018) (Weeden și Sanson (eds.) April 2021).

3. The role and place of space systems as critical infrastructure

The designation of spatial systems as critical infrastructure depends primarily on the extent to which such systems and assets are so vital to a country that their incapacity or destruction could seriously affect the national security, economic security, the public health and safety or any combination thereof. Therefore, experts should establish the degree of dependence of different areas of activity of the economy and society on the specific services and products offered by these space systems.

Space systems and assets have become indispensable for the efficient functioning of various applications and services in the civil (commercial and scientific) and military fields or the protection of Earth from meteoroids and space debris. The malfunctioning of space systems can have detrimental consequences for industry and agriculture, the energy sector, transport, banking and financial system, military operations, government activities and therefore the well-being and security of the population. For example, the banking sector uses Global Positioning System (GPS) to time-stamp the financial transactions, precision agriculture uses space systems to assess the existence of variables, such as status of soils, planting density, fertilizer spreader, crop yield estimation, and other applications including rail traffic control, highway traffic management, commercial aviation and maritime navigation depend on satellites for location and operational safety (Piso 2015, 15). The economy and energy systems also depend on the proper functioning of space systems for resource mapping services, management of pipelines and other industrial facilities, and vital services, such as supply of energy and drinking water, information and communication technologies and even waste management depend directly on them.

Last but not least, space and space technologies are a topic of great interest to military planners, given that the operating environment will be characterized in the near future by the innovation and operationalization of capabilities specific to new areas of military operation (cyberspace and outer space) (Romanian Ministry of National Defence 2021, 9). Therefore the space systems must be considered from a dual perspective – both the advantages of these technologies in the civil and military spheres, as well as the potential threats and risks to national security. They are a key factor in gaining superiority on the battlefield and should be integrated into all joint operations, both as a facilitator and as a force multiplier.

Undoubtedly, space systems are essential and affect the functionality of other critical infrastructure sectors. Space assets are critical because they are part of the various applications and systems that affect everyday life and national security, from satellite television, GPS systems, and the constellation of satellites that will provide worldwide broadband internet, to high-speed communications and early warning of ballistic missile attacks. In fact, thousands of low-orbit Earth satellites will help develop new 5G networks, large-scale information infrastructures and global connectivity to IoT.

The most recent assessments of the US Intelligence and National Security Alliance have identified several reasons why space systems should be designated as the 17th critical infrastructure sector. For example, in support of national security, commercial satellites have detected new intercontinental ballistic missile sites in China, provided valuable information to disaster response actions, and found some signs of potential collisions along the India-Pakistan border, tracked piratery, poaching and illegal fishing activities (Intelligence and National Security Alliance November 2021, 4). Other possible missions of commercial geospatial systems relate to space imaging, intelligence gathering, disaster prevention and preparedness, search and rescue, weather forecasting, communications.

The designation of space systems as a new category of critical infrastructure will facilitate access to space and increase the security and resilience of key space systems, adding protection to production and supply chains for others satellites, spacecraft and components,

while extending existing protections for communications satellites to their launch and mission systems (Space Foundation 2021, 4). This would open up new opportunities (Swallow și Visner 2021) such as: promoting and strengthening collaboration in the space industry, on the one hand, and between industry and government authorities, on the other (more specifically between manufacturers, suppliers, owners and operators); developing basic space and counter-space systems; fostering the achievement of a global consensus on the essential nature of space assets and the need to protect and support them; identifying and developing a system for assessing threats and risks to space systems; and accelerating the adoption of best standards, practices and technologies for securization and resilience of space systems.

The US has already taken the first steps in the process of designating the space systems as a critical infrastructure sector (Waterman 2021), given the fact that dependence on space assets is greater than ever before and access to space is vital to the national and economic security, whether we're talking about the United States and its allies, or China, Russia and India.

Conclusions

Today, the space environment is particularly complex and dynamic, consisting of civil, commercial and military systems on which we are increasingly dependent. No country that wants to expand its economy and strengthen its national security can ignore outer space and space systems as a source of data and information, a channel of communication and an area of potential risks and threats. Competitive advantage is about adapting to new strategic challenges by developing new sophisticated space systems and technologies, in which satellites are, if necessary, tools for multiplying forces – continuous global coverage, low vulnerability, autonomous operations – and can provide essential secure communication about weather conditions, navigation data and possible threats.

Space systems are therefore critical due to their place and the role they play in the stability and functionality of the political, economic, social and military system system, by the degree of exposure to certain disruptive factors, but also by the variable set of their vulnerabilities to threats that directly or indirectly target them. Under these conditions, the designation of space systems as a new sector of critical infrastructure becomes mandatory, so that states and regional organizations can coordinate policies, strategies, programs or resources in support of these space systems and set clear security and resilience standards for them.

BIBLIOGRAPHY:

BEARSE, Ronald S. 2021. "An Overview of Critical Infrastructure, its Importance, and Key Policy Terms." *Terrorism Experts Conference "The Military Role in Countering Terrorism"*. Edited by NATO Centre of Excellence Defence. Ankara, Turkey, October 12-13. Accessed November 19, 2021. https://www.tmmm.tsk.tr/TEC2021/presentation/Ronald%20BEARSE.pdf

European Commission. 2006. *Communication from the Commission on a European Programme for Critical Infrastructure Protection.* Brussels, December 12. Accessed November 19, 2021. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

European Commission. 2005. *Green Paper on a European Programme for Critical Infrastructure Protection.* Brussels, November 17. Accessed November 19, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN

Intelligence and National Security Alliance. November 2021. "Designating the U.S. Space sector as Crtical Infrastructure." Accessed December 15, 2021. https://www.insaonline.org/wp-content/uploads/2021/11/INSA_WP_Space_v3.pdf

Joint Chiefs of Staff. 10 April 2018. "Space Operations." Joint Publication 3-14.

KYLE, Ed. 2021. ”Space Launch Report.” *2021 Launch Vehicle/Site Statistics.* December 31. Accessed January 5, 2022. https://spacelaunchreport.com/log2021.html

O’HANLON, Michael. September 2018. *Forecasting Change in Military Technology, 2020-2040.* Foreign Policy at Brookings.

PISO, Marius-Ioan. 2015. "Infrastructurile critice spațiale: introducere în securitatea planetară." *Prelegere cu prilejul decernării titlului de Doctor Honoris Causa Scientiarum al Universității de Vest din Timișoara.* December 10.

RAJU, Nivedita. 2021. *Russia’s anti-satellite test should lead to a multilateral ban.* Edited by SIPRI. December 7. Accessed December 17, 2021. https://www.sipri.org/commentary/essay/2021/russias-anti-satellite-test-should-lead-multilateral-ban

Romanian Ministry of National Defence. 2021. "Strategia Militară a României (Military Strategy of Romania)." Bucharest.

SELLERS, Jerry Jon. 2015. *Understanding Space: An Introduction to Astronautics.* Fourth Edition. New York: McGraw-Hill Companies.

Space Foundation. 2021. "The Authoritative Guide to Global Space Activity." The Space Report, Space Foundation.

SWALLOW, Edward, and Samuel Visner. 2021. "It’s time to declare space systems as critical infrastructure." *Politico.* February 4. Accessed November 25, 2021. https://www.politico.com/news/2021/04/02/its-time-to-declare-space-systems-as-critical-infrastructure-478848

The White House. 2003. *Homeland Security Presidential Directive/Hspd-7 - Critical Infrastructure Identification, Prioritization, and Protection.* December 17. Accessed November 17, 2021. https://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html

The White House. 2013. *Presidential Policy Directive/PPD-21 - Critical Infrastructure Security and Resilience.* February 12. Accessed November 17, 2021. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The White House. 2003. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* February. Accessed November 17, 2021. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

2021. *UCS Satellite Database.* September 1. Accessed October 12, 2021. https://www.ucsusa.org/resources/satellite-database

United Nations Office for Outer Space Affair. 1966. "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." December 19. Accessed November 16, 2021. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

United Nations Office for Outer Space Affairs. 1979. "Agreement Governing the Activities of States on the Moon and Other Celestial Bodies." December 5. Accessed November 16, 2021. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html

US Congress. 2001. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001." *Public Law 107-56.* October 26. Accessed November 17, 2021. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

US Department of Defense. January 2011. "National Security Space Strategy."

US Office of Homeland Security. 2002. *National Strategy for Homeland Security.* July 16. Accessed November 17, 2021. URL: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

WATERMAN, Shaun. 2021. *DHS Weighs How to Protect Increasingly Critical Space Systems.* Edited by Via Satellite. November 19. Accessed December 16, 2021. https://www.satellitetoday.com/cybersecurity/2021/11/19/dhs-weighs-how-to-protect-increasingly-critical-space-systems/

WEEDEN, Brian, and Victoria Sanson (eds.). April 2021. *Global Counterspace Capabilities: An Open Source Assessment.* Secure World Foundation.

DOI: 10.53477/2668-6511-22-18

CYBERGEOPOLITICS AND CYBERGEOSTRATEGY – EMERGING STUDY FIELDS

Marius-Cristian NEACȘU, Ph.D.,
Associate professor, Bucharest University of Economic Studies, Romania.
E-mail: marius.neacsu@ase.ro

Ioana-Andreea CHICIUC,
Master Student, Bucharest University of Economic Studies, Romania.
E-mail: a_chiciuc@yahoo.com.

Abstract: *For some time now, mankind has entered a new phase of evolution, with physical space (land, sea, air, cosmic) being doubled by the virtual one, cyberspace – the global network of interconnected information technologies – and geopolitics and geostrategy could not fail to take into account this new phase in the evolution of history, with the emergence of subfields such as cybergeopolitics and cybergeostrategy, with some authors already anticipating cybernetocracies or cyber powers. It should only be added that cyberspace can be both an environment for the 'new' power (the geopolitical logic being the same) and a weapon – the cyberweapon (the use of cyberattacks as a geostrategic tool). The aim of this study consists in identifying the main components (definition, subject matter, terminology) of the two emerging areas, namely* cybergeopolitics *and* cybergeostrategy. *The results of this qualitative research are based on the critical analysis of the specialized literature, in order to summarize the specific phenomenology and to theorize the concept of cybergeopolitics and its dervates.*

Keywords*: cybergeopolitics; cybergeostrategy; cyber power; cyber security; cyber war.*

Introduction

Context. Starting from the assertions of the German philosopher Herder – "History is geography in dynamics" (Neacșu 2018, 177) – the mastermind Romanian scientist, Simion Mehedinți, founder of modern geography as science and as university subject, and at the same time the one who conducted the first geopolitical analysis in our country, had the great idea ("the great intuition", in his own words), of the "geographical phases of history" (Mehedinți 1940), which he developed in a number of studies and scientific communications throughout his life (Neacșu 2018, 129). Thus, the following phases have been completed so far:

I. *The continental phase*, which from a geopolitical and historical geography perspective corresponds to the continental powers (ancient cities, ancient empires, medieval empires, continental powers in modern history and today: Russia, Germany, etc.) – the so-called *tellurocracies*; it is the longest period of geopolitical evolution of all; the essence of a continental power was theorized within the Anglo-Saxon school of geopolitical-geostrategic thinking (see also Neguț 2015), through the theory of continental power or the theory of the *heartland*, with Halford Mackinder's contribution, since 1904, with the concept of the geographical pivot of history;

II. *The maritime/oceanic phase*, followed the continental phase, overlapping it, highlighting the maritime powers (*the thalassocracies*), the colonial empires and modern maritime powers such as the United Kingdom and the USA; maritime powers were superior to

continental powers, given the predominance of water over land, and *sea power theory* was conceptualized by Alfred Mahan in 1890;

III. *The aerial phase* of history has diversified the attributes of power of the two previous dimensions, with the addition of airspace domination, which has led to a conceptual reconfiguration at geopolitical and geostrategic levels; the leading air powers (*aerocracies)* were the two cold War superpowers, USA and USSR, and at theoretical level Carl Schmitt stood out with the theory of the aerocracy.

IV. *The space phase* followed naturally after the aerial phase, with two distinct temporal dimensions: a) traditional space powers (*spatiocracies*) during the Cold War (USA and USSR), to which others have joined (China, Japan, India, etc.) and b) an emerging phase, a new space race, which is very recent and different from the one during the Cold War, by its commercial and private nature and many other aspects, which involves many emerging states (UAE, Turkey, Israel, etc.) and non-state actors (private companies – SpaceX, Blue Origin, Virgin Galactic and others, foundations, various entities, eccentric billionaires, etc.); the conceptualization of new notions, which capture the ongoing phenomenology, was made, among others, within the Master in Geopolitics and Business. (Bucharest University of Economic Studies), with concepts such as *exoeconomics* (Șapera 2015, 2013), *exopolitics*, *exostrategy* and *exobusiness* (Șapera 2021, Neacșu and Matei 2021) or *exoturism* (Neacsu 2021, in press).

V. *The cyber phase* is the most recent, with cyberspace being global despite its virtual nature, the effects of its manifestation are as territorial as possible, causing conceptual metamorphoses, such as *cybergeopolitics* and *cybergeostrategy* (Neacsu and Chiciuc 2021, 66-71).

The aim of this study is therefore in line with the previously developed phenomenological context, particularly the current phenomenology of the cyber phase of history, and consists in identifying the main components (definition, subject matter, terminology) of two emerging areas, namely *cybergeopolitics* and *cybergeostrategy*.

The novelty of the research is obvious, all these concepts highlight an ongoing phenomenology in a sharp dynamic: from using cyberspace as an environment for power manifestation (whoever is not present in cyberspace is not present in the "big chess" power games, the phrase used by Zbigniew Brzezinski 2000 or the "world scene" in Malița 2007) to turning cyberspace into a geopolitical tool: cyber weapon (and possibilities for use are vast in today's hybrid world).

The study is *innovative* by the concepts analyzed, proposing a new terminology and an attempt to theorize the concept of *cybergeopolics* and everything related to it.

The applicative character of the paper is implicit, in addition to the theoretical contributions, the enrichment and updating of the literature in accordance with the dynamics of the present reality, the study is also a theoretical guide to understanding a phenomenon which is currently in full swing.

1. Cyberspace – the new dimension of geopolitics and geostrategy

As geopolitics refers to the use of the geographical factor in maximizing power, and geostrategy refers to the implementation of geopolitical theory, the new environment of action, the cybernetic one, could not remain exclusively as technological support in the field of "civil" activities, as long as any asset means, from a geopolitical perspective, a step in overcoming the opponent and a better position towards regional or global domination. Especially in the context of the pandemic in the last two years, when almost everything has moved to the online space and digital dependence is growing.

This new reality must be understood in two dimensions: 1. the conflict with a geopolitical nature, despite its substratum which is extremely "territorial", physical, concrete,

has now acquired a digital dimension and 2. the digital space is both the environment for the manifestation of power, as well as the instrument itself, as a cyber weapon, with tangible effects, in the physical, geographical space.

The relevant published literature has captured this transition in various words, labelling cyberspace as "the digital face of geopolitics" (Kausch 2017, 2) or "the fifth dimension of geopolitics" (Barrios 2019), "the fifth element of the new world" (Refoyo 2018 quoted by Barrios 2019) or, continuing the great idea from Simion Mehedinti, "the fifth phase of history", i.e. the fifth evolving phase of geopolitics (see also Neacșu and Chiciuc 2021, 67).

As regards cyberspace, its definition has evolved in parallel with its better understanding from "consensual hallucination" and "unthinkable complexity" (Gibson 1984, 37) to "the nervous system – the country control system... composed of hundreds of thousands of interconnected computers, servers, routers, switches and cables made of optic fibre that enable our critical infrastructures to work" (Kuehl 2009). We notice the phrase "critical infrastructures" and the concern for its vulnerability (thus a possible target for the enemy, who might be tempted to consider it as such) are emphasized along with the link between the virtual environment and the reality from the field. The last author further nuances the specificity of virtual space, i.e. "a global domain in the information environment (...) to create, store, modify, exchange and exploit information through interrelated and interconnected networks using information communication technologies" (*Ibidem*).

More recently, the virtual space was defined as "the global network of interconnected IT technologies: hardware, software, information, which hosts some of the most powerful weapons, as well as vulnerabilities of the states" (Segal 2016 cited in Kausch 2017, 2). This applies to all the global actors and parties which are interconnected to this global network which gives cyberspace the quality of being "the vanguard of future geopolitical confrontations" (*Ibidem*). In other words, interdependence (economic and military) – mainly theorized by the liberal school of thought in international relations ("mutual dependence" in Joseph Nye jr. or "interdependence" in Robert Keohane) – has moved into the virtual space and has become a cyber-interdependence (Neacsu and Chiciuc 2021, 68).

In summary, cyberspace has become a *space for the manifestation of power*, maintaining the classical geopolitical and geostrategic logic (maximum destruction with minimal losses, preeminence in front of the opponent), and a new *atribute of power – cyber power*.

These interconnected and interdependent networks and information systems are simultaneously located in both the physical and virtual space and within and across geographical borders. The notions of "space", "time", "distance", "border", "identity" and so on have changed drastically, technical developments and the great advancement of artificial intelligence have created a framework for the emergence of a new type of conflict – *cyber conflict* – which adds to the traditional component of "hybrid", "atypical" or simply "unconventional".

By continuing this hypothesis, cyberspace can become a weapon that gives even small states or smaller geopolitical actors greater power and combat capacity, substantially changing the notion of "asymmetric conflict" (see also Harari 2015, 20-21). Relevant and recent examples of this are the terrorist organization Islamic State (ISIS, which operated in Syria and Iraq, with its recent version of ISS-K, in Afghanistan after the withdrawal of US troops and the international coalition in mid-2021) or the Taliban.

If against a state actor there is a legal framework and an international response mechanisms, against volatile entities that act through cyberspace, it is very difficult to react. In other words, the power monopoly of the nation-state is relative. Since the late '90s and especially since the mid-2000s, when cyber attacks against states have increased, governments

started to see cyber threats as a national security problem (Desforges 2014, 67-81), while some analysts had already announced early on the possibility of cyberwar (Arquilla and Ronfeldt 1993, 141–165).

Viewed as a 'battlefield' (Ministère des Armées 2013, 38) or 'confrontation field' (*Ibidem*, 45), cyberspace has become the vector of cyber threats. These cyber threats have evolved from cyber crime to cyber geopolitics, namely through the use of cyber attacks as a foreign policy tool (cyber weapon). The most vulnerable to cyber threats are the most developed countries, due to the high degree of interconnectivity between computer networks. Seen as a nation's "nervous system" (Kuehl 2009), networks have become a vital challenge for governments, which have placed *cyber security* or *cyber defense* as a component of national security (Cavelty 2008).

2. Cyber power

In traditional or conventional geopolitics, the following are included among the main attributes of high power (see also Neguț 2015): economic power, military power, nuclear power, cosmic power, membership of various international bodies, such as permanent membership of the UN Security Council.

Considering that more than 75 billion devices were connected to the internet in 2020, interconnecting almost 3 billion people (around 35% of the world's population), a new attribute of great power is emerging: *cyber power* (Neacșu and Chiciuc 2021, 68). The element that makes cyberspace give such power is the interdependency and interconnectivity network that it creates, with our current life being almost inseparable from it.

However, as a particular study (Kuehl 2009) points out, the problem is not controlling electrons or electromagnetic forces, but rather influencing the use of cyberspace, in the same way that airborne or naval superiority does not concern the control of air or water molecules, rather, it controls how they are used in the physical environment. Thus, according to the same study, the definition of cyber power is that *"cyber power is the ability to use cyberspace to benefit us and to influence events in all operational environments and among all other power tools"* (*Ibidem*).

From a military point of view, cyber power has been the most influential instrument in the last two decades. From the Russian concept of *military technical revolution* (Kurtinevich Jr. 2002) in the 1980s, to the transformation of US military defense, cyberspace and cyber power have been at the heart of new concepts and doctrines of the last decades. Cyber power has become an indispensable element of modern technology-based military capability because it occurs across all the levels of conflict.

As it was mentioned before, what is different from the traditional geopolitics is that cyber power is not accessible only for the big powers, small states or non-state actors also being able to access it, thus making the cyber dimension a true geopolitical tool.

3. The cyber weapon. Cyberwar. Players. Towards conceptualizations of cybergeopolitics and cybergeostrategy

It should be noted that the use of the *cyber attack* is also based on hard power logic, the military invasion of geopolitical and traditional geostrategy being replaced by cyber attacks, either to cause a breach in the opponent's network and to obtain data (digital espionage), or to cause considerable damage (therefore as a digital weapon). The cyber weapon did not replace conventional weapons, but joined them in the battlefield, imprinting the *unconventional (hybrid)* character into conflicts.

Although the recorded cases are already well-known for a long time (the US cyber attacks against Serbia in the ‘90s, the cyber attacks on Estonian public and private institutions in 2007, the Russian cyber attacks in the 2008 war with Georgia, etc.), some authors consider 2012, as the "year 0" of the cyber war (more specifically, the timeframe between June 2012 and June 2013, where information was leaked in the media), when the US, together with Israel, resorted to a cyber attack against Iran's nuclear program (since 2010), using a malware called Stuxnet and compromising the program that was controlling the centrifuges of uranium enrichment facilities. The effect? At least 1 000 engines operating the centrifuges were destroyed (by sudden acceleration and deceleration). The Iranian cyber response came without delay, a group called Izz ad-DIN al-Kassam attacked 50 US financial institutions, which spent around $10 million to get back online (Segal 2016). The era of cyber warfare had begun: the use of the cyber weapon was producing physical damage (in the case of the engines from the Iranian centrifuges and more), with the associated costs...

As a result, cyber defense has become one of the main topics on NATO's public agenda, with the organization stating that "international law applies to cyberspace" (NATO 2020), with Bucharest being chosen to host a European Cybersecurity competency Center as of 2021. A cyberspace that is regulated internationally is thus introduced by a series of "rules" (Ruhl et al 2020), being a "strategic domain" (Popa 2014), with geopolitics and geostrategy now taking a mixed approach, both physical and cyber (Oxford Analytics 2018). And Henry Kissinger, the well-known US diplomat and the "spiritual parent" of a famous "Diplomacy", said "Cyberspace is beyond any historical experience. (...) The threats that come from cyberspace are diffuse and difficult to ascribe" (Kissinger 2014).

Cyber attacks have significant advantages in a conflict compared to conventional instruments. They have high disruptive potential and have a relatively low economic cost for the attacker. The political cost in the form of a risk of retaliation is also low, given the difficulties that arise in tracing the offender. The problem of author identification is perhaps the most acute and presents a real challenge for traditional disincentives (Kausch 2017).

The concept of war is used to describe a diverse set of conditions and behaviors, from a state of violent and armed escalation (such as classical wars) to symbolic disputes or disagreements, which are far from the real meaning of this concept. The concept of cyber war has also been used to describe different situations, ranging from credit card fraud or a campaign of cyber vandalism and cyber-space disruption, to a real state of war conducted by cyber means. (Singer and Friedman 2014, 120).

According to the US Government, in order to turn into cyber war, a cyber attack must cause injuries, significant destruction or even death. While the means of doing this are in cyberspace, they must have physical damage (*Ibidem*) in the real world. *Cyberwar* is thus defined as *the use of cyber attacks to attack a state or disrupt vital information systems, causing damage comparable to real war* (NATO 2013). There is significant debate among experts on the definition of cyber war. One view is that the term "cyber war" is incorrectly used, as no cyber action to date could be described as war (*Ibidem*). An alternative perspective is that cyber war is an appropriate label for cyber attacks that cause physical damage to people and objects in the real world (Lucas 2016).

Hard-power manifestations in cyberwar are generally represented by attacks conducted in the cyber space designed to produce political effects similar to those of conventional wars (Lucas 2017), but elements of hard power such as military intervention, economic sanctions and coercive diplomacy are replaced by elements of cyber war, such as cyber attack, cyber espionage or state-funded *hacktivism*.

McAfee, a cyber security firm published the *Cyber crime report in 2009* under the title *Virtually here: The age of Cyber Warfare*, in which it included a world map of countries that were developing advanced cyber capabilities at the time. The title of the map was: *Cyber war*

is not taking place today, but states are definitely in competition (Kurtz 2009). This report estimated that there were only about twenty countries, which actually have advanced cyber-war programs and could build something comparable to the Stuxnet virus.

Additionally, some current "major players" inside the cyberspace have been stepped up (Segal 2016), respectively some *cyber powers* – states that use the cyber dimension to increase their competitive advantages as players on the global stage - such as USA, Russia, China, Germany, Brazil, Israel. In addition to those listed, we can add other cyber actors, including Japan, North Korea, Iran, Vietnam, India, Pakistan, etc. (University of Pittsburgh Institute for Cyber Law, Policy and Security 2019).

The complex nature of cyberspace involves several representations, which shape government strategies in this new power environment. In such cases, these representations become geopolitical instruments. For example, Russia has omitted the direct use of the term cyberspace, instead opting for the term "*informational space*". By using this broader concept, Russia is not only limited to the classic idea of cyber attacks, but is choosing strategies that aim at more widespread information control, regardless of their channel of distribution (Desforges 2014, 67–81).

As it is not a physical space, cyberspace is viewed by geopolitical actors as a virtual world generated by the interconnectivity of the Internet network. However, geopolitical conflicts that use cyberspace as a vector of manifestation, and which are, among other things, the focus of cybergeopolitics, are real and reflect the rivalries between states that exist outside the virtual world.

In an article from 1997 entitled *Internet géopolitise le monde*, it was mentioned that "instead of making geopolitical conflicts more difficult to take place, the Internet seems to multiply and complicate them" (Douzet 1997, 222–233), the standard notions from the geopolitics field, such as power, influence and conflict are also "altered" by the new cyber dimension.

As a result, given what has previously been mentioned, the subject of cybergeopolitics studies becomes cyberspace, i.e. the way it works as an amplifying environment for power (in which geopolitical actors are confronted), but also the way it becomes a geopolitical tool (the cyber weapon).

Thereby, *cybergeopolitics* is individualized as the newest geopolitical subbranch, which analyzes *the movements of forces of global actors in the cyberspace, the motivations/interests behind these movements and their impact on relations between actors in the global dynamic*. In addition, *cybergeopolitics* can be used alongside *cybergeostrategy* to study the instruments of *hybrid war*.

Regarding terminology, it has become widely diversified in recent years, with specialized terms coming into existence starting from cyber space such as *cyber threat cyber crime, cyber terrorism, cyber risk, cyber security, cyber diplomacy, cyber intelligence, cyber conflicts, cyber war* etc. (Neacșu și Chiciuc 2021, 68).

Furthermore, the related phenomenology is also quite diverse, from simple *disinformation* and the spread of *fake news* to *cyber attacks* against critical infrastructures of other states. If cybergeopolitics sets the goal that needs to be achieved, cybergeostrategy provides the path (tactics, strategies) for achieving that goal.

Conclusions

Analysing the tendency of theoretical conceptualization of the two emerging fields – *cybergeopolitics and cybergeostragy* – the following have been reached:

1. The cybernetic phase is a new stage in the geopolitical evolution of humanity. Continuing the idea of the "geographical phases of history" of the great scientist Simion Mehedinți, we find that humanity has entered a new "era", in which cyberspace has become

predominant in all aspects of life. From a geopolitical point of view, the emergence of "cyber powers" (*cyberocracies*) is foreshadowed, just as each major phase of evolution has generated continental (*tellurocratic*), maritime (*thalasocratic*), air (*aerocratic*) or spatial (*spaceocratic*) powers.

2. Cyberspace is the fifth dimension of geopolitics and geostrategy. The role of the geographical factor in maximizing power (control of land, seas and oceans, air, circumplanetary space) has been completed with a new dimension, the cybernetic one, which adds strengths in addition to the previous ones. Being a complex global network, based on interconnectivity and interdependence, cyberspace also presents vulnerabilities, which can be speculated to cause damage, including physical ones. In addition, the inexorable accessibility to the virtual space with minimal costs maximizes the number of potential geopolitical actors, state and non-state, in addition to the already established great powers.

3. Cyber power is a new attribute of great power, in addition to those already known, namely economic, military, nuclear, space power or membership in various international bodies such as permanent membership of the UN Security Council. In essence, cyber power captures the ability of an actor to "navigate" the cyber environment and explore its attributes, turning it into a *cyber weapon*, such as, for example, initiating cyber attacks on critical infrastructures in another state.

4. Cyber conflict originated from the conventional one, attributing to a modern conflict the *hybrid* or *atypical* or *unconventional* label. Thus, theoretically speaking, the translation from the *hard power* to the *hard cyber* can be observed, retaining the geopolitical logic of intervention and force manifestation, but changing the instrument (tanks invasion was replaced by fake-news invasion, as a *softer* version or even actions with results that lead to material damage such as cyber attacks).

5. Cybergeopolitics is an emerging area that seeks to capture the new ongoing phenomenology, with cyberspace as the "study object", in two ways: as *an environment for the manifestation of power* and as *a tool of power* (the cyber weapon). In this context, specialized terminology has enriched itself with new words such as *cyber threat, cyber crime, cyber terrorism, cyber risk, cyber security, cyber diplomacy, cyber intelligence, cyber conflicts, cyber wars*, etc.

6. Cybergeostrategy is a natural extension of cybergeopolitics and consists of applying the theory and achieving its objectives. Therefore, both cybergeopolitics and cybergeostrategy provide the tools for the study of hybrid war.

BIBLIOGRAPHY:

BARRIOS, Miguel Ángel. 2019. "Cyber-geopolitics: a strategic analysis from our America." Accessed October 2, 2021. URL: https://www.vision-gt.eu/news/cyber-geopolitics-a-new-field-of-study-to-understand-the-attacks-to-critical-infrastructure

BRZEZINSKI, Zbigniew. 2000. *Marea tablă de șah. Geopolitica lumilor secolului XXI,* București: Ed. Univers Enciclopedic.

CAVELTY, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age,* London: Routledge.

DESFORGES, Alix. 2014. "Les représentations du cyberespace: un outil géopolitique." *Hérodote* 152-153, no. 1-2: 67–81. URL: https://www.cairn.info/revue-herodote-2014-1-page-67.htm

DOUZET, Frédérick. 1997. "Internet géopolitise le monde." *Hérodote* 86-87, no. 1-2: 222–233.

GIBSON, William. 1984. "Neuromancer." Accessed October 2, 2021. URL: http://index-of.es/Varios-2/Neuromancer.pdf

HARARI, Yuval Noah. 2015. *Homo deus: scurtă istorie a viitorului*. Iași: Ed. Polirom.

KAUSCH, Kristina. 2017. "Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East." Accessed October 2, 2021. URL: https://www.gmfus.org/news/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east

KISSINGER, Henry. 2014. *World Order*. New York: Penguins Books.

KREPINEVICH Jr., ANDREW F. 2002. *The Military-Technical Revolution: A Preliminary Assessment*. Washington: Center for Strategic and Budgetary Assessments. URL: https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf

KUEHL, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem" In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, ch. 2. Lincoln: University of Nebraska Press. URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

KURTZ, Paul B. 2009. "Virtual Criminology Report 2009: Virtually Here: the Age of Cyber Warfare." Accessed October 2, 2021. URL: https://media.hotnews.ro/media_server1/document-2009-11-17-6518495-0-virtual-criminology-report-2009-virtually-here-the-age-cyber-warfare.pdf

LUCAS, George. 2016. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press.

LUCAS, George. 2017. "State-Sponsored Hacktivism and «Soft War»." *Civil American* 2, art. 2: 1–6. URL: https://goo.gl/R55J4V

MALIȚA, Mircea. 2007. *Jocuri pe scena lumii: conflicte, negocieri, diplomație.* București: Ed. C.H. Beck.

MEHEDINȚI, Simion. 1940. "Fazele geografice ale istoriei. Observări geopolitice" In *Opere Complete. Vol. 1, Partea a II-a*, edited by Simion Mehedinți 1943, 308–319. București: Fundația Regală pentru Literatură și Artă.

Ministère des Armées. 2013. *Le Livre blanc sur la défense et la sécurité nationale*. Paris: Direction de l'information légale et administrative. URL: https://fr.calameo.com/read/000331627d6f04ea4fe0e

NATO. 2013. "Cyberwar – does it exist?" Accessed October 2, 2021. URL: https://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html

NATO. 2020. "Cyber defence." Accessed October 2, 2021. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm

NEACȘU, Marius-Cristian and Chiciuc, Ioana Andreea. 2021. "Conceptul de geopolitică cibernetică (cybergeopolitics)." *Terra* LI (LXXI), no. 2: 66–71.

NEACȘU, Marius-Cristian and Matei, David. 2021. "Concepte emergente: exopolitică, exostrategie, exobusiness" In *30 de ani de la sfârșitul Războiului Rece*, edited by Marius-Cristian Neacșu, 156–175, in press. București: Ed. ASE.

NEACȘU, Marius-Cristian. 2018. *Simion Mehedinți și geopolitica românească*. București: CD Press.

NEGUȚ, Silviu. 2015. *Geopolitica*. București: Meteor Press.

Oxford Analytica. 2018. *Cybersecurity & Geopolitics*. Oxford: Oxford Analytica. URL: https://www.oxan.com/media/2150/oxford-analytica-cybersecurity-and-geopolitics.pdf

POPA, Iulian. 2014. "Cyber geopolitics and sovereignty. An introductory overview" In *Proceedings of The 5th International Scientific Conference National and International Security 2014, 2nd-3rd October*, edited by Armed Forces Academy of General Milan Rastislav Štefánik 2014, 413–417. Demänová: Academy of General Milan Rastislav Štefánik.

RUHL, Christian, Hollis, DUNCAN, Hoffman, WYATT, and Tim MAURER. 2002. *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Washington: Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/files/Cyberspace_and_ Geopolitics.pdf

ȘAPERA, Andrei. 2013. "Towards Exoeconomics – Developing an off-planet economy and its implications." Accessed October 1, 2021. URL: http://www.fgdb.ro/ assets/resurse/Andrei-Sapera-Exoeconomics-2013.pdf

ȘAPERA, Andrei. 2015. "Exoeconomie. Dezvoltarea economiei extraplanetare" In *România noului val*, edited by Marius Stan, Bogdan Gravrilă, 357–363. Bucharest: Civil Society Resource Center.

ȘAPERA, Andrei. 2021. "Exostrategy and Space Industry 4.0." webinar, March 9 and April 6. Bucharest University of Economic Studies (MA Geopolitics and Business).

SEGAL, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. London: Hachette UK. URL: https://books.google.ro/ books?id=LDxWDgAAQBAJ&printsec=frontcover&hl=ro&source=gbs_ge_summary_ r&cad=0#v=onepage&q&f=false

SINGER, P.W. and Allan Friedman. 2014. *Cybersecurity and cyber war – what everyone needs to know.* New York: Oxford University Press.

University of Pittsburgh Institute for Cyber Law, Policy and Security, US Government and others. 2019. "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar." Accessed October 1, 2021. URL: https://www.dhs.gov/sites/default/files/ publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

DOI: 10.53477/2668-6511-22-19

NUCLEAR PROLIFERATION AND THE CENTRAL BALANCE: STRUCTURAL SCENARIOS

Mihai Vladimir ZODIAN, Ph.D.
Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania.
E-mail: zodian.vladimir@unap.ro

Abstract*: This paper synthetizes earlier studies and aims to investigate how the nuclear equilibrium between the United States and the Russian Federation may change, because of the process of proliferation*[1]*. A theoretical perspective combining power transition and rational deterrence theory is used to draw a few scenarios. The main goal is to develop general traits and tendencies, by varying the variable of power distribution and use them to develop a few scenarios.*

Keywords*: Nuclear weapons, nuclear balance, power transition, deterrence, nuclear strategy, rise of China, prediction.*

The theme`s importance comes from a few generally accepted ideas on nuclear technology and its consequences. First, the destructive potential and the general belief in the stabilizing effect which they may have upon Great Power relationships are making debates about nuclear weapons still relevant, even after the end of the Cold War and the fall of the Soviet Union. There are also issues the rise or return of China as a great power, including its modernization of the armed forces and the debates on the expansion of the nuclear arsenal. In the academia, the theories about power, armaments and deterrence are controversial and incomplete; thus, any discussion can be useful, and their practical recommendations should be approached with prudence, especially about prediction and concrete policy advice[2].

Theoretical prediction based on structural analysis is the main method used here. According to the chosen perspective, a few transforming tendencies will be sketched. The epistemological quality of this is speculative, but it may serve some practical needs. For example, how to employ theories to understand better reality and to imagine forms of change, which helps to better cope with it (Chernoff 2012; Zodian, 2015).

This paper is divided in three sections. In the first one, the concepts of equilibrium and proliferation are analyzed, and their characteristics and ambiguities are detailed. Next, a discussion on power transition and rational deterrence theory follows. The last section holds the scenarios, based on the earlier discussion.

1. What is changing?

The term equilibrium is notoriously ambiguous (Haas 1953; Wight, 1998)[3]. In nuclear strategy, the most important distinction to be made is the one between parity and vulnerability (Schelling, [1966] 2008, loc 181; Bull, 1998; Buzan 2000; Keohane and Nye 2009). A consequence of the difficulty of defense and of the destructibility of weapons, this reflects the

[1] The paper resumes the study Mihai Zodian, *Proliferarea nucleară și echilibrul strategic central în secolul* XXI, Editura UNAp, 2020.
[2] See also the discussion about balancing from Vasquez and Elman 2012.
[3] For the issue of measuring power, see Miroiu 2005 and Baldwin 2016.

classical debate between power and security. Power focused explanations, like offensive realism and some versions of transition theory will emphasize primacy, superiority or general equality, while security-focused ones, vulnerability and survivability (Mearsheimer, 2001; Kugler and Zagare, 2008; Waltz 2006; Wohlstetter 2009).

One may start from the basics. In terms of deterrence, the main point is to make a credible threat that presses the opposing side to retreat from an unwanted action, which means that the concept of vulnerability to a response is more important that power in general (Art, 2000). One usually deters by superior force, and this is the message of power transition theory and law enforcement, but the characteristics of nuclear weapons brought a change here, if the consequences are feared and impossible to avoid. Deterrence requires, according to Morrow a military capability, which can exploit this weakness, a clear signaling of intention and that the intention to use the force is believed by the potential challenger, the last two parts enouncing the problem of credibility (Morrow, 2000).

The issue is still controversial. Rational deterrence theory relaxes the assumptions of rationality or perfect information to avoid the paradox that, since the costs are so high either to challenge, or to deter, the whole questions look irrational (Morgan 2003). This is like the paradox of voting, where people vote, even if instrumental comparisons of benefits suggests that they should abstain, but with the difference that deterrence theory is both descriptive and prescriptive, and influenced policy (Downs, 2009; Morrow 2000). Many solutions were proposed, a recent one in the form of risk propensity and Bayesian estimation of credibility (Zagare and Kilgour, 2000), which mixes power with vulnerability; for the purpose of this paper, a classical version of the theory will be used, based on Schelling idea of a threat that leaves something to chance (Schelling, 2000).

There are also many versions of deterrence postures (Narang, 2014). The typical classification, according to the goals pursued, finds minimal deterrence; assured destruction and more ambitious capabilities, ranging from denial to warfighting (Viotti, Kauppi 2013, 307-314; Narang, 2014). Even if the force in being is just a part, and the relationship is psychological in great part, different combinations were proposed and linked to distinct types and degrees of stability. While mutual assured destruction (MAD) was often highlighted and recommended, the other options found supporters, and this led to another unsettled series of debates[4].

Therefore, the concept of nuclear equilibrium does necessarily imply parity or identity of forces and strategies. This view, based on security concerns, and close to the idea of assured destruction, is contrasted with the fact that superpowers often wanted equality or parity in forces or power, not just an admission of unavoidable vulnerabilities (Mearsheimer, 2003). While the drive failed in the sense that redundant capabilities were built, it nevertheless motivated, at least formally the policies pursued by some major actors and may be important in the medium or long term again. Thus, the contemporary nuclear relationship is a combination of ambitious forms of deterrence with formal parity (Narang 2014).

The historical dimension is also significant. The specific postures, capabilities and strategies often changed, especially during the Cold War, which lead to the definition of a central equilibrium between the United States and the Soviet Union, now Russia. While the forces were drastically reduced, the general configuration is still comparable, with the two actors on top, and several others with small arsenals. Since 1945, proliferation was slow compared with the potential, but worries lately were expressed towards the goals of Chinese modernization program, whether it has abandoned minimum deterrence in favor of assured destruction or is it interested in a more ambitious design (DoD 2021).

[4] Postures are connected, but not identical with strategies like countervalue, counterforce, first strike etc.; see

This section investigated some of the ambiguities in the ideas of central nuclear equilibrium. The most important is the ambiguity and the risk of confusing the reciprocity of vulnerability with ideas about parity between forces and states. A major disequilibrium may refer to the acquisition of an assured destruction capability by a new nuclear power; the buildup of a massive nuclear arsenal by a previous owner, or the various forms of arms control, disarmament and technological change; I opt for the meaning distinguished by Narang, of big arsenals, available for multiple missions, including assured destruction, to the Great Powers, right now, to the United States and Russia (Narang, 2014). The next segment of this paper holds the theoretical framework.

2. Why is changing?

Alterations of the distribution of capabilities are often brought about by arms races and military revolutions (Waltz 2006). Unfortunately, these two phenomena are not very well understood, especially on how to conceptualize them and how to link them with the occurrence and character of war and other possible consequences. For the subject of this paper, is also often confusing those similar issues are approach differently under the label of deterrence and nuclear proliferation, two areas which are close and share similar causal mechanisms. For example, scholars who belief that deterrence policies are stable tend to be more phlegmatic about horizontal proliferation (Waltz 1981).

Understanding arms races is part of this commonality. Buzan distinguished between competitions and dynamics, the first one referring to special contests, involving unusual interactivity and costs, while the second is a contrast, the normal workings of the international system. Allison underlined the value of understanding the internal characteristics and politics of the actors, in his classic (Allison, Zelikow 2010). A.F.K. Organski and Jacek Kugler showed that arms expenditures don`t show interactivity, even in the case one may expect that, such as during the Cold War, between the United States and the Soviet Union, proposing one of Allison`s models, the organizational one (Organski, Kugler 1980).

The research expanded further. Other authors used theories about norms culture, symbolic interactions, international diplomacy and sanctions, or economic globalization, but there are still unanswered questions (Solingen 2007; Tannenwald 2009; Narang 2017). One example: under which conditions, a political regime dedicated to growth and welfare who forswears or downplays the role of nuclear weapons may change his strategy? Or, if one considers variables like the international pressures or nuclear postures, as proposed by Narang, the decision to get requires a different explanation.

This line of thinking puts parsimony under question and is difficult to apply. A general approach is needed, but without going too far from the facts, especially since arms dynamics are not autonomous processes, easy to distinguish from political or economic factors (Waltz 2000). Therefore, it will be used a combination between power transition theory and the classical version of rational deterrence theory. The first is a partly structural theory and is useful in building scenarios, because just a few conditions need to be varied; the second avoids the confusion between mutual vulnerability and parity mentioned above.

Power transition theory assumes that certainty leads to peace and ambiguity to war (Vasquez 2009, 57-58). Scholars in this tradition, like Frank Zagare and D. Marc Kilgour approached nuclear weapons like any other type of weaponry, and tried to dismantle rational deterrence theory, arguing that is based on an equality of capabilities. Their proposal, perfect (consistent) deterrence argues that this supposed parity should lead to war, because any of the actors involved may win, an uncertainty related to the result, which can be avoided by a strong nuclear imbalance of capabilities or perceptions (Zagare, Kilgour 2004). But a similar and reciprocal type of vulnerability is not parity and can lead to both clarity and stability, especially if the states can`t guarantee that they keep full control during crises or limited wars (Schelling 1967; Walt 1999).

Therefore, power transition rational deterrence theory and can be combined, considering their limits. The first one explains war between major powers and rivalry in general based first on the (rapid) catchup of a previously dominating actor by one or more challengers and second, on the rulers' dissatisfaction with the existing international order (Organski, Kugler 1980; Soare 2013). Since parties are becoming comparable in capabilities, any of them has a fair chance to win a war. This uncertainty causes the conflict and is compatible with both explanations in terms of a security dilemma and with James Fearon's model of war, as shown by Woosang Kim and James Morrow`s analysis (Kim, Morrow 1992; Fearon 1995).

The result is underdetermined in two directions. From an operational point of view, the degree of satisfaction is difficult to estimate in a quantitative methodology as the one preferred by power transition`s theorists. Thus, testing involving mostly capability measure show that the power distribution may be a necessary cause, but is not sufficient to cause conflict and war, since in many cases, the parties found a settlement (Vasquez 2009). It`s also unclear whether the confrontation should arrive at the beginning of transition, in a preventive war, or close to its end, since the timing depends on the stakes, credibility and negotiations (Kim, Morrow 1992).

These issues of causality suggest that an actor-level interpretation is also needed. Now, rational deterrence theory argues that the power transition should be mostly peaceful because the results are easy to predict and very costly (Waltz 1981; Quackenbush, Zagare 2017). By contrast, the perfect deterrence conceptualization shows that, even with nuclear weapons, there is a considerable risk of war if parties are determined to fight, or they are particularly good at bluffing (Zagare, Kilgour 2004). Thus, the chosen perspective makes a stark difference in threat-assessment.

In this section, some conceptual issues about arms races and nuclear proliferations were reviewed. I argued that a theoretical choice was needed and that the difference is meaningful concerning the conclusions and evaluation. A combination between power transition and rational deterrence explanations was proposed as a solution for the question of prediction. As with any structural interpretation, the precise results are underdetermined, as shown by Kim and Morrow in this case (Kim, Morrow 1992), but the general traits of international system are vastly different, according to the theory employed, and this is the next section`s subject.

3. How is it changing?

Any prediction requires to keep some issues constant. In this case, I consider that the international system won`t undergo a fundamental change in principle, type of units or the logic of action. The main idea of this section is to use theoretical prediction, and structural variables to see how the central equilibria may change, a method often employed by neorealists like John Mearsheimer or by power transition theorists like Kugler; the central nuclear equilibria mean here the vast arsenals, capable of multiple missions, retained by the US and Russia after the Cold War (Vasquez 2009; Kugler, Tammen 2009; Mearsheimer; Narang 2014). The specific distribution of power will be varied, in unipolar, bipolar and multipolar, at the systemic level, to generate scenarios, using power transition theory to link structure to the range of anticipable outcomes.

The first scenario is about unipolarity, the system dominated by one power. This means that United States will remain the foremost power, either by good policy, or by a combination of circumstances, including bad management by China`s political leaders (Organski, Kugler 1980; Kugler, Tammen 2009). It`s the most peaceful future, if we talk about great power relationship, according to the perspective used in this paper. It`s also the most conservative, and easy to question version.

In this case, how can the central equilibrium change? The baseline expectation is that we shouldn`t see much of it, since, by definition, there isn`t much use for nuclear weapons, except simple forms of deterrence. The reason is that only one power is capable of global military action, including to protect its allies. Nevertheless, there are a few venues of change: a regionalization of international political system; a reduction of concentration of power in the system, between the pole and competitors; intense nationalism or domestic interests; nevertheless, the best policy in this type of configuration remains to keep the arsenals low or to make a deal with the superpower (Buzan, Waever 2004).

The second scenario is about bipolarity. In this case, there is a distribution of power in which the United States and a second actor, China most likely, are comparable in terms of capabilities. There are several versions, especially the distinction between tight and flexible variants, according to the degree of hostility and pattern of alliances. Seeing from the perspective of power transition theory, it`s the most problematic political configuration, in which rivalry may lead to crises and local wars, and the international system is divided between the two poles (Organski, Kugler 1980; Kugler, Tammen, 2009).

It`s also an exceedingly popular idea, in the recent years, as argued by many, including Allison with his famous Thucydides trap (Allison, 2017). Especially in tight bipolarity, there are intense structural stimuli for a challenger like China to develop a massive nuclear arsenal, for both prestige and security reasons; the system may be stable or highly conflictual according to a variety of factors, including the beliefs about deterrence (Kaplan 1957) The central nuclear equilibria may become like a balance with three pans, quantitatively and very complex, looking from the vantage of vulnerabilities; for example, the relationship between China and Russia may also influence its configuration, or the rivalry between Beijing and Washington may be less important in the nuclear area (Organski, Kugler 1980; Kugler, Tammen, 2009). In flexible bipolarity, a massive arsenal should be either unlikely or embedded in various arms control regimes; the regional decentralization and deconcentration options are still available.

The third scenario is about multipolarity. In this alternative, there are at least three or four global powers, and with flexible and ambiguous political relationship. It is usually divided in classical multipolarity; Congress type of orders and division in rival alliances polarization, mostly based on modern European history, but other examples can be found (Kaplan 1957). For power transition theory, is a risky and prone to war international distribution of power, but the concrete results may be more temperate, due to different threat perceptions.

In this narrative, the central nuclear equilibria may change, especially if the international system is polarized in two main blocks. The main reason is that alliances are flexible and extended deterrence requires special policies to keep credibility, which means more missions and objectives for a nuclear capability (Organski, Kugler 1980; Kugler, Tammen, 2009). In the classical multipolarity, smaller arsenals and more horizontal proliferation are more probable, since there are more stimuli to pass the buck, as argued by Christensen and Snyder, while a Congress-like order can control the spread of this type of armament. The regionalization possibility collapses in the rest of categories, in this case (Christensen, Snyder 1990).

There are also scenarios in which the distribution of power is less important. For example, a generalized deterrence system based on assured destruction (Kaplan 1957; Waltz 1981); the opposite, a general disarmament; the decline of any of the two major nuclear powers or technological change. They aren`t the focus in this paper but is important to be aware of the many other alternatives. Their probabilities seem to be low.

Conclusions

There are still ambiguities in the use of the balance or equilibrium metaphors in International Relations. For the topic approached here it is important to notice and underline the oscillation between vulnerability and equality when discussion the situation of the United

States and Russia. The meaning employed here includes both deterrence based on assured destruction and significant dimensions. This vagueness will probably remain in the literature.

The theoretical perspective combined power transition and rational deterrence theory. An idea rejected by some power transition theorists, it offers enough simplicity to deploy structural analysis and narrate a few major scenarios. Power transition argues that imbalance of capabilities leads peace, offering a way to link structure to results. Rational deterrence theory simplifies the choice of variables.

The main scenarios followed the three classical international systems. The bipolar version is the most unstable, according to the theory, and a power like China may pursue the developing of a vast nuclear arsenal. The multipolar system comes next, in which more countries may be involved in complex rivalries. The unipolar seems to be the more stable, taking great powers relationships into account; there are different variables for each, according to institutionalization and degree of hostility.

BIBLIOGRAPHY:

ART, Robert. 1980. "To What Ends Military Power". *International Security*. 4(4): 3-35.

BALDWIN, David A. 2016. *Power and International Relations. A Conceptual Approach*, Princeton: Princeton University Press.

BULL, Hedley. 1998 [1977]. *Societatea anarhică. Studiu asupra ordinii în politica mondială*, Chișinău: Editura Știința/CEU Press.

BUZAN, Barry, WAEVER, Ole. 2004. *Regions and Powers. The Structure of International* Security. Cambridge: Cambridge University Press.

BUZAN, Barry. 2000 [1991]. *Popoarele, statele și teama*. Chișinău: Editura Cartier.

CHERNOFF, Fred. 2012. *The Power of International Theory. Reforging the Ling to Foreign Policy-Making Through Scientific Enquiry*. London, New York: Routledge.

CHRISTENSEN, Thomas J., and SNYDER Jack. 1990. "Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity". *International Organization* 44 (2): 137-168. doi:10.1017/s0020818300035232.

DoD. 2021. *Military and Security Developments Involving the People`s Republic of China 2021. Annual Report to the Congress*. Office of the Secretary of Defense.

DOWNS, Anthony. 2009 [1954]. *O teorie economică a democrației*. Iași: Institutul European.

GRAHAM Allison, ZELIKOW T., Philip D. 2010 [1971, 1999]. *Esența deciziei. O explicație a crizei rachetelor din Cuba*. Iași: Polirom.

GRAHAM Allison. 2017. *Destined for War: can America and China escape Thucydides`s Trap?* Boston: Houghton Mifflin Harcourt.

HAAS, Ernst B. 1953. "The Balance of Power: Prescription, Concept, or Propaganda", *World Politics*. 5(4): 442-477.

KAPLAN, Morton A. 1957. *System and process in International Policies*. Wiley: New York.

KEOHANE, Robert O., NYE, Joseph S. Jr. 2009 [1977]. *Putere și interdependență*. Iași: Polirom.

KIM, Woosang, MORROW, James D. 1992. "When Do Power Shifts Lead to War?". *American Journal of Political Science* 36 (4): 896.

KUGLER, Jacek, TAMMEN, Ronald L. 2009. in William R. Thompson (ed.), *Systemic Transitions. Past, Present, And Future*. New York: Palgrave MacMillan.

KUGLER, Jacek, ZAGARE, Frank C. 1990. "The long-term stability of deterrence", *International Interactions*, 15(3-4), pp. 255-278, DOI: 10.1080/03050629008434733

MEARSHEIMER, John J. 1990. "Back to the Future: Instability in Europe after the Cold War". *International Security*. 15(1): 5-56.

MEARSHEIMER, John J. 2003 [2001]. *Tragedia politicii de forță*. Bucuresti: Antet XX Press.

MIROIU, Andrei. 2005. *Balanță și hegemonie*. București: Editura Tritonic.

MORGAN, Patrick M. 2003. *Deterrence Now*. Cambridge, New York: Cambridge University Press.

MORROW, James D. 2000. "The Ongoing Game-Theoretic Revolution". In Midlarsky, Manus I. (ed.). *Handbook Of War Studies II*. Ann Arbor: University of Michigan Press.

NARANG, Vipin. 2014. *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict*. Princeton: Princeton University Press.

NARANG, Vipin. 2017. "Strategies of Nuclear Proliferation: How States Pursue the Bomb". *International Security* 41 (3): 110-150. doi:10.1162/isec_a_00268

ORGANSKI, A. F. K, KUGLER, Jacek. 1980. *The War Ledger*. Chicago: The University of Chicago Press.

QUACKENBUSH, Stephen L., ZAGARE, Frank C. 2017. "Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies". *Oxford Handbooks Online*, May 2016, DOI: 10.1093/oxfordhb/9780199935307.013.39

SCHELLING, Thomas C. 1967. *Arms and Influence*, Yale University Press, Kindle edition, 1967.

SOARE, Simona. 2013. "Tranziția de putere". In Biró, Daniel. 2013. *Relații internaționale contemporane*. Iași: Editura Polirom.

SOLINGEN, Etel. 2007. *Nuclear Logics: Contrasting Paths in East Asia and Middle East*. Princeton: Princeton University Press.

TANNENWALD, Nina. 2009. *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945*. Cambridge: Cambridge University Press.

VASQUEZ, John A., ELMAN, Colin (eds.). 2012 [2003]. *Realismul și balanța de putere*, Iași: Polirom.

VIOTTI, Paul R., KAUPPI, Mark V. 2013. *International Relations and World Politics*. Boston: Pearson.

WALT, Stephen M. 1999. "Rigor Or Rigor Mortis? Rational Choice and Security Studies". *International Security* 23 (4): 5-48. doi:10.1162/isec.23.4.5

WALTZ, Kenneth N. 1981. "The Spread of Nuclear Weapons: More May Be Better: Introduction". *The Adelphi Papers* 21 (171): 1-1. DOI: doi:10.1080/05679328108457394

WALTZ, Kenneth N. 2000 [1954]. *Omul, statul și războiul*. Iași: Institutul European.

WALTZ, Kenneth N. 2006 [1979]. *Teoria politicii internaționale*. Iași: Polirom.

WIGHT, Martin. 1998. *Politica de putere*, Chișinău: Arc.

WOHLSTETTER, Albert. "Theory and Opposed-Systems Design", In Zarate, Robert. Sokolski, Henry (eds.), 2009. *Nuclear Heuristics: Albert and Roberta Wohlstetter*, Carlisle: The Strategic Studies Institute.

WOHLSTETTER, Albert. 1959. "The Delicate Balance of Terror". In Zarate, Robert. Sokolski, Henry (eds.), 2009. *Nuclear Heuristics: Albert and Roberta Wohlstetter*, Carlisle: The Strategic Studies Institute.

ZAGARE, Frank C. KILGOUR, D. Marc. 2004. *Perfect deterrence*. Cambridge: Cambridge University Press.

ZODIAN, Mihai. 2015. *Perspective epistemologice și predicții în relațiile internaționale*. București: Editura Universității Naționale de Apărare „Carol I".

ZODIAN, Mihai. 2020. *Proliferarea nucleară și echilibrul strategic central în secolul XXI*, București: Editura Universității Naționale de Apărare „Carol I".

DOI: 10.53477/2668-6511-22-20

TOWARDS AN EU STRATEGIC CULTURE: THE CHALLENGE OF RECONCILING NATIONAL CHARACTERS AND A COMMON EU SECURITY AND DEFENSE POLICY IN THE BLACK SEA

Olga R. CHIRIAC,
Associated Researcher, Center for Strategic Studies,
National University of Political Studies and Public Administration, Bucharest, Romania.
E-mail: olga.r.chiriac@gmail.com

Abstract: *In the current global context of great power competition and while fighting to overcome and recover from the COVID-19 pandemic, the EU has embarked on the ambitious undertaking to redefine itself as a more capable, credible, independent when necessary, defence stakeholder, the EU strategic autonomy process. Throughout this endeavour, it is becoming more and more apparent that one of the more challenging dimensions of the EU strategic autonomy debate is dial of national characters and strategic cultures within the union. The aim of the paper is conceptualizing the strategic culture framework in EU context and to identify both positive and negative factors that carry the potential to influence the formation of an authentic European strategic culture. The final conclusions will assess whether any subsequent actionable policy is in fact possible in the foreseeable future, mainly to what extent an autonomous European strategic culture could act as either a facilitator or inhibitor of EU security and defence decision making.*

Keywords: *Black Sea; European Union; strategic autonomy; strategic culture.*

Introduction

The concept of strategic culture appears more and more in the field of strategic studies. It is especially the case for the European Union (EU) ever since the union embarked on the strategic autonomy process. Talk about a more self-sufficient EU in the field of defence is nothing new, however, in the most recent years it became a decade priority. The principal aim of the article is to conceptualise the strategic cultural framework in EU context, how or if strategic culture impacts strategy and the strategic choices made in Brussels, in particular. The conclusions should be able to differentiate whether the concept acts as facilitator or inhibitor at the political-decisional level in Brussels as it relates to a common EU security and defence policy in the Black Sea. The paper is not looking to conduct an all-encompassing analysis of the concept of strategic culture by investigating the theoretical explanatory powers of the term: does it possess the capability to explain at least to some extent the relationship between strategy and national inclinations for security and defence behaviour, or is it for the most part nothing more than another intellectual justification for security and defence policy choices. Such an endeavour would be beyond the limited scope of the paper.

The paper is structured as follows: first a brief discussion around the chronology of the concept in international relations literature, second a concise presentation of the EU strategic environment, finally, the case study brings the findings down to an important strategic space in the EU security and defence architecture – the Black Sea. The paper emphasizes the role of perceptions and national strategic cultures by underlining the difference in EU security and defence posture in the Black Sea by focusing on the evolution of EU political initiatives in the

region. Finally, we are talking about the North Atlantic Treaty Organisation's (NATO) Eastern Flank in an analysis about EU strategic thinking because, at this point in time, although the EU has developed into a regional political-economic institution with military ambitions, the alliance remains the de facto defence provider for the European Union in its entirety.

1. Strategic Culture – A Framework for Analysis

In spite of a truly vast amount of literature covering the topic, there is no relative academic consensus as to the ontological dimension of strategic culture. Each attempt to a definition either adds another layer or expands already convened on taxonomy.

Strategic culture was first coined by Jack Snyder and defined as "the sum total of ideas, conditioned emotional responses, and patterns of habitual behaviour that members of a national strategic community have acquired through instruction or imitation and share with each other" (Snyder 1977, 8). Nevertheless, the origins can be traced back to the "national character studies" of the 1940s and 1950s. These "represented some of the first social scientific efforts to draw connections between culture and state behaviour based largely on anthropological models." (Lantis 2005, 1). National character studies postulated that the core of a nation, the nation's character, stems from a nation's language, religious beliefs, customs, socialization patterns, as well as the interpretation of common memories (Elkins&Simeon 1979, 127-12). One significant element of the Snyder definition is the strategic culture aspect and it warrants the inquiry into whether the European Union has succeeded in forming one or if it remains at the aspirational level. Ken Booth defined strategic culture as "a nation's traditions, values, attitudes, patterns of behaviour, habits, symbols, achievements and particular ways of adapting to the environment and solving problems with respect to the threat and use of force" (Booth 1990, 121). Values, beliefs, attitudes make their way into the definition, behaviour remaining a constant. Stephen Rosen characterized strategic culture as a concept which incorporates "beliefs and assumptions" which in turn have an impact on "choices about international military behaviour, particularly those concerning decisions to go to war, preferences for offensive, expansionist or defensive modes of warfare, and levels of wartime casualties that would be acceptable." (Rosen 2019, 12). The general agreement is that strategic culture references the behavioural choices by states as they relate to the threat or use of force. In this sense, states are strategic actors. Another general agreement is that the concept of strategic culture stems from the concept of political culture. (Gray 1984, 27). Analysing through the lens of strategic culture means to assert that changes in the interaction system are not addressed objectively but rather through the "perpetual lens provided by the strategic culture." (Gray 1984, 27). The evidence used in constructing the concept includes both words and actions, "declaratory material" such as leadership speeches and declarations and military doctrinal documents or military and political activity. Colin Gray labelled the resulting political activity and policy as strategic behaviour, or" behaviour relevant to the threat or use of force for political purposes." (Gray 1999, 50). Naturally, strategic culture and national character are not fixed concepts. They transform and are fully dynamic. More recently, there have been frequent calls for a EU "strategic concept" (van Staden et al., 2000; Biscop, 2002; Fiott, 2020), "which would set out the EU's objectives in the field of security and defence as well as a strategy of how to achieve them." (Meyer 2004, 2). In the academic debate, strategic culture is employed in foreign policy analysis in order to explain the behaviour in security and defence of either states and/or international organization. In the context of the paper strategic culture is a framework for analysis for the European Union Common Security and Defence Policy and as a measure of how the EU is looking to define itself as a strategic actor: does strategic culture act as a variable which facilitates or inhibits the development of an authentic, autonomous common security and defence policy. Is there real progress in developing an EU strategic culture?

The strategic culture conversation in EU context makes even more sense when tied into the evolution of European security and defence policy planning and execution. The Saint-Malo declaration in 1998 marked the birth of the European Security and Defence Policy (ESDP). A few years later, the European Union Military Committee (EUMC) was set up within the EU Council (EU Council Decision of 22 January 2001) and in 2003, the EU formalized the common European Security Strategy, a policy document looking to develop an EU strategic culture "which fosters early, rapid, and earn necessary, robust intervention" (EU 2003, 11). In 2009, the Lisbon Treaty offered the opportunity for even greater cooperation on multilateral responses through a Common Defence and Security Policy (CSDP) framework. It is the European Council through unanimous decision who identifies strategic interests and objectives of the EU. The CSDP has "greatly evolved since the entry into force of the Treaty of Lisbon, both politically and institutionally" (EU Parliament, 2021). The ultimate goal is to achieve a "policy setting the EU's framework in the field of defence and crisis management, including defence cooperation and coordination between Member States" (EU Parliament, 2016). CSDP and the ESDP both drew the outlines for the European Union as a security actor and this translates into a union of joint security interest and the ways to protect them. Notably, cooperation in security and defence and integration of security and defence structures are two very different concepts.

Strategic culture in the context of the present article is convened upon as playing a role in the deeper understanding of "motivations, self-image and behaviour patterns of decision-makers", it "helps shape" but "does not determine how an actor interacts with others in the security field" (Booth 2005, 25). Specifically, national strategic cultures do exist, however, we need to analyse whether they have a positive or negative effect towards the development and progression of an EU strategic culture.

To sum up, strategic cultural analysis has certainly gained traction in the international relations field of research. Pioneered by Lack Snyder in the late 70's, at the high of the Cold War, strategic culture has started out mostly as a concept meant to build explanatory theories for soviet strategic behaviour, especially in the nuclear realm. In time, the concept was rediscovered and extended to all other actors in the international system. Concurrently, the definition of security widened and the strategic environment became far more complex, especially due to globalization and the significant progress made in technology innovation. For the purpose of the article, the concept of strategic culture will be employed as a tool to explain state behaviour and an attempt will be made to reconcile it with the union of states which is the EU.

2. EU, the Strategic Actor

The strategic environment the EU is operating in has changed dramatically in the last decades, in the post-Cold War era. In the field of security and defence, national characters and national strategic cultures did not carry much traction during the Cold War. Strategic cultures developed organically at the national level, however, the world was ordered in a bipolar manner, and major strategic decisions were reached depending on the elegance of each state to either the East or the West, the USSR or the USA, the two superpowers. Present day EU is a conglomerate of 27 Member States, the union is one building block in a multipolar international system, where since the December 2017 US National Security Strategy great powers are officially back to systemic competition. While one political and economic block, in the field of defence, the union has fallen short of reaching a unitary position. Although the international system has changed, becoming far more interconnected and complex, each Member State remained heir to distinct national perspectives rooted in history, geography, culture, and geopolitics.

There is no genuine shared perception of threats in the EU yet, no authentic consensus as too what makes the union vulnerable security wise. The EU Strategic Compass currently underway in Brussels is meant to map out a clearer direction as well as spell out the threats the union is facing. The EU remains an emerging strategic actor in the realm of security and defence not a fully formed one. It remains to be seen what the Compass will lead to as far as actionable policy. Recent reports about the Strategic Compass draft say that the EU is considering the formation of a joint military force of up to 5,000 troops by 2025 to intervene in a range of crises and without relying on the United States (US News, 2021). This is indeed very good news, nevertheless, it will hopefully not suffer the same fate as the battlegroups. In 2007 with "the introduction of the Battlegroup concept, the Union formed a (further) military instrument for early and rapid responses when necessary." (EU Council, 2013) The concept reached full operational capability on January 2007, full operationalization and application lagged. Notwithstanding, as of right now, while at the declaratory level the member states agree on the imperative of developing a more autonomous EU in security and defence, and while the EU institutions work on setting up the necessary institutional framework, the means to reach such a goal, the reality on the ground remains fragmented. Different geographical areas have different strategic interests and security is often still ensured by bilateral strategic partnerships, and, as stated before, NATO. For example, on the Eastern border of the EU, Poland and Romania rely heavily on their strategic partnership with the US as well NATO. Strategic culture is correlated to political culture and political culture is rooted in the historical memory of each nation. This is a substantial roadblock in establishing a common EU strategic culture. According to the present framework for analysis, political leadership of a state and the political elites are the decision makers when it comes to policy and strategic direction. They are the ones shaping narratives, public discourse and this in turn influences that way states behave as strategic actors. In order to form a total strategic actor, the EU needs to meet both requirements: agree on the political ends and construct the necessary means to reach those ends. The later part could in fact constitute a major advantage for the EU on the world stage because the union is a wealthy institution with substantial economic means. The European Defence Fund (EDF) is the best example of said power. Unfortunately, the bottleneck remains at the political level, where the consensus is not there. A major step in reaching a consensus was indeed the initiation of the EU Strategic Compass, the two-year process, led by the European External Action Service under the responsibility of the EU high Representative for Foreign Affairs and Security Policy (EU External Action Service, 2020). In addition to mitigating the fact that the EU lacks a common strategic culture, the compass is intended to morph into a "new security policy document" and it "must be based on a broad political consensus and a strong political will to act." (EU German Presidency Website, 2020). The Strategic Compass will address different, inter-linked areas: crisis management missions, resilience, capabilities and instruments, working with partners. A target adoption date is March 2022, under the French Presidency. It remains to be seen if the target date will be met and if indeed the compass will produce progress.

Practically, a very recent example of the EU as strategic actor is the evolution of the allied withdrawal from Afghanistan. The North Atlantic Treaty Organization (NATO)–led International Security Assistance Force (ISAF) in Afghanistan was established by the United Nations in 2001. (NATO, 2021) The declared main purpose was to train the Afghan forces as well as to assist in rebuilding government institutions. This NATO led mission included armed forces from several EU nations and, based on the premise of common historical experiences, would have been the perfect opportunity for the different states to start building a common strategic answer, a shared way of viewing military missions, their purpose. In August 2021, during the hasty western withdrawal from Afghanistan, the common EU strategic response simply did not exist. Mary Kaldor wrote about the missed opportunity to build an EU response in a moment of crisis: "A European force that remained even as the Americans left could have

provided a powerful psychological boost to Afghan forces – and such an operation should have been well within European capabilities." (Kaldor, 2021) One option would have been to keep EU forces on the ground, however, the political will, the EU consensus was just not there. An EU strategic culture has remained an ambiguous concept, which different meanings for different groups. This is just a very recent example. Of course, it would be reductive to evaluate the EU potential to morph into a truly strategic actor by just one occurrence, nevertheless, it provides a good insight to the situation at present. The current migrant crisis at the Poland Belarus border is another opportunity, so far, it looks like Poland considers invoking NATO Article 4, no clear expression of support from Brussels. According to the Polish News Agency, European Council President Charles Michel said that the EU together with Member States and the European Commission will consider measures that are "significant and tangible" in impact(PAP,2021) One such measure is apparently funding infrastructure of the EU's eater border. Physical structure on the borders in order to protect the bloc is not a strategic answer. The root cause of the threat is not addressed.

To conclude, the EU is an emerging strategic actor, however, it has a way to go before reaching synergy. The good news is that the right steps at the political level are being taken, the more realistic news is that in spite of several security documents and political initiatives, the on the ground reality tells a different tale. Perhaps Berger's view that strategic culture is best understood as a "negotiated reality" among foreign policy elites is most fitting to describe the present phase in EU's pursuit of a common strategic culture.

3. EU Strategic Presence in the Black Sea Region

Barry Buzan and Ole Wæver concluded "Most threats travel more easily over short distances than over long ones" (Buzan & Wæver 1998, p. 4). The Black Sea and the place the region occupies in EU strategic output is a fitting illustration for this assertion. The union's strategic approach towards the Black Sea Region reflects in how initiatives have materialized or not in the past.

As a theatre of naval operations, the Black Sea represents one of the maritime borders of NATO's Eastern Flank. Access to the Black Sea is limited by narrow straits, mainly the Bosphorus and the Dardanelles. The straits are on opposite ends of the Sea of Marmara. From a maritime regime stand point, the straits as well as the Sea of Marmara are part of the sovereign maritime territory of Turkey and therefore subject to the regime of internal waters. The navigational regime regulating maritime traffic in and out of the Black Sea is the Montreux Convention of 1936. The Black Sea is a semi enclosed body of water bordered by six coastal states: Bulgaria, Romania, Ukraine, Russia, Georgia and Turkey. Three of them, Bulgaria, Romania and Turkey, are NATO member, while two of them, Georgia and Ukraine, aspire to NATO accession. Finally, Bulgaria and Romania are EU members. The annexation of the Crimean Peninsula by the Russian Federation in 2014 effectively enabled Russia's expansion of its exclusive economic zones (EEZs) and the building of the Kerch Strait Bridge in 2018 which complicated the geopolitical landscape even more.

The EU strategic approach in the Black Sea is inherently linked to the very way the EU was constructed. A political and economic union first and foremost, it took a very long time as well as substantial structural changes in the international system for her to start having serious defence related conversations , especially relating to the Black Sea. Up to the present, the strategic initiatives of the union in the BSR are largely not correlated to actionable security and defence.

Black Sea Synergy (BSS) is the main EU initiative for the region. The official launch of the initiative took place February 14, 2008, in Kiev, on the occasion of a meeting of the

ministers of foreign affairs of the EU Member States and the states in the region covered by the BSS: Armenia, Azerbaijan, Georgia, the Republic of Moldova, the Russian Federation, Turkey, and Ukraine. (MAE, 2021). BSS was launched particularly because of the strategic position of the Black Sea, "its potential in the fields of energy, transport, trade, environment, democracy building" (MAE, 2021). The declaratory interest was there, however, there lacked political follow up and there was not too much project level application.

Previously too BSS, the European Union (EU) has developed in 2003 a new working foreign policy instrument called the European Neighbourhood Policy (ENP) in order "to achieve the closest possible political association and the greatest possible degree of economic integration" with its Southern and Eastern neighbours (EU Commission, 2021). Out of the ENP came another EU political framework, the Eastern Partnership (EaP) "which Romania views as a powerful soft power instrument to anchor Eastern neighbours to EU's identity and values" (Aurescu, 2011). The Eastern Partnership was launched in 2009 and is a joint initiative involving the EU, its Member States and six Eastern European Partners: Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine. This initiative is indeed a strategic move on behalf of the EU, establishing areas of "strategic interest": Azerbaijan is rich in energy resources for example, a strategic priority for the union. On the other hand, the same initiative underscores fundamental strategic divergence among EU Member States: while Poland for instance would naturally be very interested in the EU actively supporting Belarus or Ukraine in building sound democratic systems of governance, other Member States might not share in this sense of urgency. The current migrant crisis at the polish Belarusian border is an illustration of why the EU should care. Another good example is the Republic of Moldova: while Romania is vested in Moldova's European integration, other fellow EU Member States might not consider this a strategic priority. The formation of both BSS and Eastern Partnership is indicative as to the direction in which the EU was envisioning its strategic play in the Black Sea. Both put an accent on cooperation, mainly in items at the top of EU agenda such as human rights, democracy and consolidation of democratic institutions, the economy and trade, good governance, energy, transport, climate policy, maritime policy, fisheries, human security and migration.

The European Neighbourhood Policy was intended to "to create a ring of friends around the borders of the new enlarged EU" (Ferrero-Waldner, 2004). Notwithstanding commendable goals, the EU strategic actor did not manage to properly assess the threat environment, to this day, miscalculating its policy towards the Russian Federation. The Black Sea has therefore suffered from a security and defence vantage point, the EU does not have a common approach to Black Sea security and defence aspect. Black Sea security, in spite of the geopolitical significance, is still exclusively a matter for NATO and the riparian states. EU strategic culture in the Black Sea does not have any sort of power. In both Baltic and Black Seas, the Russian Federation is the regional military power. Although NATO faces the same strategic competitor in both bodies of water, the regional threat perception is very different. If the Black Sea is characterized by tension and relative mistrust, in the Baltic, the stance is very divided. The former Baltic Republics for instance, Latvia, Estonia and Lithuania, together with Poland perceive the Kremlin as a realistic and grave threat to their national security. At the opposite end of the spectrum we have Germany, who in spite of numerous declarations condemning different forms of alleged Russian aggression, have partnered up with Russia to construct Nord Stream 2, a controversial pipeline project, feared by many states in the EU and NATO to be a strategic Trojan horse. The German answer to the concerns over Nord Stream 2 was not a European answer, individual national character has trumped the overarching EU security interest.

The Three Seas Initiative (3SI) is the most recent attempt to settle the EU into its role as strategic actor. 3SI is a" politically inspired, commercially driven platform for improving

connections among twelve EU Member States located between the Baltic, Adriatic and Black Seas" (2seas.eu, 2021). While focused on economic cooperation, in the wider context of energy and maritime security, the 3SI could very well be employed as a powerful tool in addressing EU security. It remains to be seen how this opportunity will be leveraged, not only by the participating countries, which have a strong commitment to security and defence as common denominator, but in the EU overall.

The EU strategic autonomy process, currently underway in Brussels, could be a wonderful opportunity to indeed streamline a cohesive, common strategic culture. The need for an autonomous EU is evident, it would be the needed complementarily to NATO and the immediate area of action is the EU neighbourhood. Frozen conflicts in Azerbaijan (Nagorno-Karabakh), Georgia (Abkhazia and South Ossetia), the Republic of Moldova (Transnistria) and Ukraine (Donetsk and Lugansk) are still looking for a political solution. They contribute to instability in the region, inherently threatening EU security.

The starting point of the present work was the question: does the emerging EU strategic culture act as a facilitator or inhibitor for a common EU security and defence policy? In concrete terms is the EU as strategic actor in the Black Sea? Through a strategic culture lens, the answer is negative, as well as multi-layered. The strategic cultures of different actors in the Baltic as well as the Black Seas act as inhibitors towards building a common EU strategic culture, however, in different ways. If in the Baltic Sea, there is essentially no need for a more assertive EU policy because the regional power, the Russian Federation does not perceive the EU and NATO as threats, in the Black Sea, the environment is far more complex and tense. In the Black Sea, Russian strategic thinking presents a posture build around the conviction that it is better to prevent a loss than to expect a positive outcome. While the efforts to create the ripe environment for the development of a cohesive EU strategic culture is a noteworthy one, it must be said that in order for this process to be relevant, it needs to be backed by more political will, to be more situation minded and regionally/geographically specific, and, finally, to be accelerated. In line with the latter, in his writings about strategic culture, Colin Gray was alerting to the fact that "Restrictive understanding of the strategic culture of others can be very dangerous for international peace and security". (Gray 1984, 26) It is in the interest of both the EU and NATO, for the European Union to continue the discussion and to pursue initiatives such as the EU Strategic Compass. Caveat, the compass will be rooted in threat assessments and intelligence sharing, not political national agendas, motivated by national strategic cultures. Being strategic means that the political decision makers build a long term blueprint for the EU in the defence realm, so far, the proposition has been at best short to medium term. The leaked draft of the compass mentions a target date of 2025 and this is nowhere near long term. The bigger picture of climate change, energy security, strategic rivalry with other great powers, all these aspects would need to be projected not the future and strategically addressed.

Conclusions

A truly common EU strategic culture would indeed facilitate common EU responses to regional threats as well as challenges in EU areas of interest or global threats such as climate change, terrorism, piracy, humanitarian crises, pandemics or proliferation of weapons of mass destruction. The paper set out to establish whether the concept acts as facilitator or inhibitor at the political-decisional level in Brussels as it relates to a common EU security and defence policy. It is clear the union is in the process of actively pursuing this goal and it is therefore important to analyse whether the union possess the capability to explain at least to some extent the relationship between strategy and defence behaviour, to define strategic interests with commonality or if, for the most part, it represents nothing more than another

intellectual/political justification for security and defence policy choices, mostly national ones. After a review of the way the concept has been conceptualized in specialty literature and after a brief incorporation of the concept within the EU strategic landscape, the discussion outlined how the goal of EU strategic culture is still at best emergent at worst and inhibitor of common EU security and defence policy, particularly in the Black Sea. Domestic values and norms still outweigh a unifying "EU character". The main reasons behind this unevenness is the varying levels of threat perception among EU Member States, in our case, exemplified by the way different state actors perceive the Russian Federation in the Black Sea and beyond. Political initiatives in the Black Sea have existed, however, the implication of the union as a whole was minimal at best. Nevertheless, the EU does not lack the necessary means to build capabilities, it just did not manage, at least so far, to build actionable consensus around the end goal of approaching threats to EU security in a unitarian manner.

In the overarching global context of renewed great power competition between the Russian Federation, China and the USA, it will become more and more evident that the EU will at some point operationalize the goal of a common strategic culture and autonomy.

BIBLIOGRAPHY:

AURESCU, Bogdan. 2011. "The Role of the European Union in The Wider Black Sea region", *Turkish Policy Quarterly*, Vol.10, Number 1.

BISCOP, Sven. 2002. "In Search of a Strategic Concept for the ESDP", *European Foreign Affairs Review*, 7.

BUZAN, B., WAEVER, O., DeWILDE, J. 1998. Security a new framework for analysis. Lynne Rienner.

BOOTH K. 1990. The Concept of Strategic Culture Affirmed. In: Jacobsen C.G. (eds) Strategic Power: USA/USSR. Palgrave Macmillan, London. URL: https://doi.org/10.1007/978-1-349-20574-5_8

Journal of the European Union. 2016. Consolidated Version of the Treaty of the European Union. Official URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016M/TXT&from=EN

ECKSTEIN, Harry. 1998. "A Culturalist Theory of Political Change," American Political Science Review 82.

ELKINS D.J., Simeon R.E.B. 2000. A Cause in Search of Its Effect, or What Does Political Culture Explain?. In: Crothers L., Lockhart C. (eds) Culture and Politics. Palgrave Macmillan, New York. URL: https://doi.org/10.1007/978-1-349-62397-6_2

EMMOTT, Robin. 2021. "EU to Aim for Rapid Deployment Force Without U.S. Assets by 2025, Document Says." US News, November 15, 2021. URL: https://www.usnews.com/news/world/articles/2021-11-15/eu-to-aim-for-rapid-deployment-force-without-us-assets-by-2025-document-says

European Council of the European Union, "Implementation Plan on Security and Defence". 2016. URL: https://eeas.europa.eu/sites/default/files/eugs_implementation_plan_st14392.en16_0.pdf

European Council of the European Union. 2017. "Council conclusions on progress in implementing the EU Global Strategy in the area of Security and Defense", URL: https://www.consilium.europa.eu/en/press/press-releases/2017/03/06/conclusions-security-defence/

EU External Action Service. 2013. Common Security and Defence Policy.EU Battlegroups. URL: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/esdp/91624.pdf

EU External Action Service. (2016). "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

EU External Action Service. 2016. "The Common Security and Defence Policy (CSDP)", URL: https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5392/common-security-and-defence-policy-csdp-structure-instruments-agencies_en

Dr. FERRERO-WALDNER, Benita. 2004. "Commissioner for External Relations and European Neighborhood Policy Speaking note, Press Conference to launch first seven Action Plans under the European Neighbourhood Policy. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_04_529

Franco-British Declaration on European Defence. 4 December 1998. Saint-Malo.

FREEDMAN, Lawrence. 2004. "Can the EU develop an effective military doctrine?", in Steven Everts, Lawrence Freedman, Charles Grant, François Heisbourg, Daniel Keohane and Michael O'Hanlon (eds), A European Way of War, Centre for European Reform, London.

GILPIN, Robert G. 1996. "No One Loves a Political Realist", in Benjamin Frankel (ed.), Realism: Restatements and Renewal, Special Issue of Security Studies, Vol. 5, No. 3, London: Frank Cass.

GOLDSTEIN, Judith and Robert KEOHANE (eds). 1993. "Ideas and Foreign Policy: Beliefs, Institutions, and Political Change", Ithaca, NY: Cornell University Press.

GRAY, Colin S. 1984. "Comparative Strategic Culture", The US Army War College Quarterly: Parameters 14. URL: https://press.armywarcollege.edu/parameters/vol14/iss1/13

GRAY, Colin S. 1999. "Modern Strategy", New York: Oxford University Press.

HOWORTH, Jolyon and John T.S. Keeler (eds.). 2003. "Defending Europe: The EU, NATO and the Quest for European Autonomy" (New York/Basingstoke: Palgrave Macmillan.

HOWORTH, Jolyon. 2019. "Strategic Autonomy and EU-NATO Cooperation: A Win-Win Approach", L'Europe en Formation, vol. no 389, no. 2.

JOHNSTON, Alastair. 1995. "Thinking About Strategic Culture", International Security, Vol. 19, No. 4.

JOHNSTON, Alastair. 1999. "Strategic Culture revisited: a reply to Colin Gray", Review of International Studies, Vol. 25, No. 3.

KALDOR, Mary. 2021. Autonomous in Afghanistan: How the Europeans could have stayed after US withdrawal, ECFR Council, September 13, 2021. URL: https://ecfr.eu/article/autonomous-in-afghanistan-how-the-europeans-could-have-stayed-after-us-withdrawal/

KATZENSTEIN, Peter J. 1996. "Cultural Norms and National Security: Police and Military in Postwar Japan", Ithaca and London: Cornell University Press.

KATZENSTEIN, Peter J.(ed.). 1996. "The Culture of National Security: Norms and Identity in World Politics", New York: Columbia University Press.

KATZENSTEIN, Peter J. 1996. "Introduction", in Peter J. Katzenstein (ed.), The Culture of National Security: Norms and Identity in World Politics, New York: Columbia University Press.

LANTIS, Jeffrey S. 2005. "American Strategic Culture and Transatlantic Security Ties," in Kerry Longhurst and Marcin Zaborowski, eds., Old Europe, New Europe and the Transatlantic Security Agenda.

LANTIS, Jeffrey S. 2009. Strategic Culture: From Clausewitz to Constructivism. In: Johnson J.L., Kartchner K.M., Larsen J.A. (eds) Strategic Culture and Weapons of Mass Destruction. Initiatives in Strategic Studies: Issues and Policies. Palgrave Macmillan, New York. URL: https://doi.org/10.1057/9780230618305_3

MAE. "Black Sea Synergy". 2021. URL: https://www.mae.ro/en/node/52664

MEYER, Christoph O. 2004. "Theorising European Strategic Culture: Between Convergence and the Persistence of National Diversity," Centre for European Policy Studies, CEPS Working Document No.204.

MOGHERINI, Federica, 2015. "The European Union in a Changing Global Environment. A More Connected, Contested and Complex World". Brussels, EEAS.

Polish Press Agency. 2021. Migration Crisis Aims to destabilize EU=Polish PM. November 10, 2021. URL: https://www.pap.pl/en/news/news%2C996554%2Cmigration-crisis-aims-destabilise-eu-polish-pm.html

ROSEN, Stephen Peter. 1991. "Winning the Next War", Ithaca NY, Cornell University Press,

ROSEN, Stephen Peter. 1996. Societies and Military POWER: India and Its Armies, Ithaca NY, Cornell University Press,

SNYDER, Jack. 1977. "The Soviet Strategic Culture: Implications for Limited Nuclear Operations", RAND Corporation, Santa Monica, CA, R-2154-AF

VAN STADEN, Alfred, KEES Homan, KREEMERS, Bert, PIJPERS Alfred and DE WIJK, Rob. 2000. "Towards a European Strategic Concept", Netherlands Institute of International Relations 'Clingendael', The Hague.

DOI: 10.53477/2668-6511-22-21

THE CONCEPT OF MULTI-DOMAIN OPERATIONS AND ITS MULTINATIONAL UNDERSTANDING

Crăișor-Constantin IONIȚĂ, Ph.D.,
Researcher, Centre for Defence and Security Strategic Studies,
„Carol I" National Defence University, Bucharest, Romania.
E-mail: ionita.constantin@unap.ro

Abstract: *The international competition on emerging technologies rises a new and very dangerous threat for global and regional security because of the easy access to the procurament of very high-tech and sensitive defence material. The race for who will control some domains from the future operating environment is between the United States, Russia and China, but several other state and non-state actors have reconsidered their high-tech strategies, already. It is about India, Iran, Japan, Israel and the European Union as a whole, as well as transnational terrorist and organised crime organisations or multinational companies. At the same time, the last technological developments have created a huge discrepancy in the Revolution in Military Affairs (RMA), especially because of letting far behind doctrines and the organisation of military structures for combat. This anacronism is evolving with the intent of gradually replacing regular fighters and current formations in the modern battlefield with robots/androids and joint human-machines teams. As a result, it has become imperative to develop new concepts/strategies for future conflicts that brings together all elemnts of advanced technologies and coordinates their joint acions on any potential adversary, in order to achieve a total and quick victory. This material will analyse the US Army's concept of Multi-dimensional Operatios and how it is understood at the Allied level.*

Keywords: *emerging technologies; Artificial Intelligence; machine learning; humanoid robots/androids; Multi-Domain Operations.*

Introductory landmarks

The complex and unforeseen events that took place worldwide in the last decade have changed the way of thinking and conducting military conflicts. As a result, the United States has considered that it is time for a new framework concept for the future military conflicts, a strategic approach of achieving complete victory in any type of warfare.

The many attempts and strategic experiments to develop new operational and strategic concepts are still undergoing at the levels of American military thinkers and defence researchers. At the end, only two selected concepts remained to be discussed and agreed at Pentagon – the US Army's concept of „Multi-Domanin Operations" and the US Government Agency for Advanced Defense Research Projects (DARPA)'s proposal of „Mosaic Warfare". Both strategic approaches are meant to take over the innovations and modernisations that appeared in the Military Science and Art, made by the different military philosophies, starting with Sun Tzu. At the same time, the existance of the two strategic documents created a dillema in the new military thinking between military thorists and defence researchers.

Indeed, many of the innovative ideas that characterise this new approach to the future warfare might be also found in Sun Tzu's *"Art of War".* But they were processed and adapted to the innovative tactics of the German's *"Blitzkrieg",* waged against the Allies in World War II, when an asymmetric advantage was obtained by using an overwhelming force of armor, motorised infantry, artillery and aviation, to create temporary breaches in the opponents' static defense that, in turn, was successfully exploited later.

Other military conceptual elements were taken from the *"Assault-Breaker"* strategy, being established as a compensation for the Vietnam disaster. Starting from the tank-airplane binomial of German tactics, the second generation strategy developed a first strategic framework focused on the deployment of an initial system-of-systems capability, in which air sensors and missile systems worked together to overcome, as a military power, the huge Red Army counterpart, without reaching nuclear escalation.

A third generation of US military strategy included the concept of *"Effect-Based Operations (EBO)*", which emerged from lessons learned in Afghanistan and Iraq. But the EBO concept has been adapted more to Military Operations Other Than War (MOOTW), leaving the conventional war to combine, on an ad-hoc basis, high-tech platforms and existing super-developed capabilities, with parts from already elaborated concepts and doctrines (developed for the use of each existing weapons platform), to which was also added the poor training of troops for the efficient use of those platforms. What has been preserved from EBO is represented by *"nodes"* and *"effects."*

The complex and unforeseen events that took place worldwide after 2014 demonstrated the need to change the way of thinking and conducting military conflicts. Thus, since 2015, US military leaders have considered that it is time for a new strategy for future wars, a strategy of obtaining the full victory in any kind of conflict.

In my book, *„Multi-Domain Operations Versus the Mosaic Warfare. Future Conflicts's Dillema Between Multi-Domain Operations and the Mosaic Warfare"*, published in 2021, I presented the numerous attempts proposed by American military theorists in the last ten years, starting from strategic concepts – *„Army After the Next"* (2010), *„Capstone Concept for Joint Operations"* (2012), *„Army Operating Concept"* (2014), *„AirLand Battle"* (2015), or *„US Marine Corps Operating Concept"* (2016) and ending with *„Multi-Domain Battle"* (2017). All these newly proposed concepts had in common the desire of military leaders to change the way of thinking and conducting future conflicts, after the operationalisation of Russian and Chinese Anti-Access/Aerial Denial systems (A_2/AD), which prevents the US from intervening in regions controlled by Moscow and Beijing.

The main idea arising from the continuity of those operational concepts was the existence of a *"man-machine"* team to fight successfully in future wars. The idea was taken from the book *"Average is Over"* of the American writer Tyler Cowen, in which machines always beat the great masters of chess, but a joint action of the chess player with the machine against another machine has great chance of success. Another idea was to realise a real synergy between multi-domains of action, by ensuring the complementarity of defense capabilities and not increasing their number, leading to an increased efficiency of their use whilst covering existing vulnerabilities, which, in turn, leads to the achievement of integrated actions of joint forces as one.

In order to develop a new strategy for future wars, the US Army launched, few years ago, the *"Multi-Domain Battle 2017"* concept for changing the way of thinking and conducting future conflicts, with the aim of penetrating enemy's A_2/AD systems and restoring the freedom

of strategic action in regions controlled by Moscow and Beijing. One year later, in 2018, scientific researchers from DARPA proposed a new strategic approach, called *„the Mosaic Warfare"*, to bring together all battle platforms to establish a complete picture of a quick and decisive victory against any aggressor, as well as to develop an appropriate package of skills. Both initiatives presented new operational concepts that would allow all joint weapon systems to work together, thus massing the fire and not the forces, in order to solve the complexity of modern operating environment and transform it into an asymmetric advantage.

1. The Development of the Concept

Starting with 2016, Army military theorists were very much focusing on solving the challenges to achieve cross-domain synergy through assessing and solving the luck of desired expertise needed, training and education shotfalls, manning, and classification and compartmentalisation of capabilities. The final result was to consider *"cross-domain synergy as a people problem"* (McCoy 2017, 4), a real constrain of having the right people, training, equipment, and doctrine to win the 21st Century Warfare.

Also, in my book I described the concept of *"Multi-Domanin Battle"*, which was launched one year later. This initial concept was designed to present the new perspective of how US military fights, both in purpose and design, to respond to the new challenges of incorporating technological advancements and diffusion, leveraging weaponised information and addressing potential adversaries' disruptive political aims designed to upend the current international order. It is already considered by US military commanders that potential adversaries have now the capability to prevent US forces from gaining access into the thater, fix them by limited US maneuver capabilities, and fracture their interdependent joint forces. (McCoy 2018, 1)

In the Concept Vision 1.0 *"Muti-Domain Battle: Evolution of Combined Arms for the 21st Century"*, the art of realising cross-domain synergy is related to the convergence and integration of systems. The convergence is defined as *"the integration of capabilities across domains, environments, and functions in time and physical space to achieve a purpose"* (McCoy 2018, 2), whilst the integration of systems is focusing not just on the people and processes, but the technological solutions required to achieve the respective synergy. (Ionita 2021, 11)

It is woth mentioning that current work in cross-domain synergy fails to aknowledge that existing systems and programmes of record are stove-piped and federated to the point that cross-domain maneuver and fires would require a human solution. So far, the lessons learned from Afghanistan and Iraq demonstrates that US military continues to fight as a large expeditionary force, massing forces in forward support areas in the theatre, with training and exercises designed to deter and prepare for the fights to come. Their lethality is unmacthed with deployed capabilities, becoming a weakness which is well-known and exploited by adversaries.

At the same time, the important notions of the Military Art – like space and time, deep, close and rear –, has evolved and today's modern operating environment became simultaneously expanding and compressing, increasing the complexity by which the war can be fought. The distance/space factor might reduce the limiting effect if we can engage lethal and non-lethal fires from anywhere around the globe. This is the case of increasing the number and importance of space and cyber-based capabilities, which can generate lethal and non-lethal

fires anywhere around the globe. Their effects have almost near-instantaneous impacts without consideirng the geographic space and political boundaries.

As Mr. Work presented during his speech at the US Army War College on 8 April 2015, "the combination of guided munitions and informationalized warfare - being able to kill by signature alone -, is a critical variable for military success in twenty-first-century warfare. Informationalized warfare is the combination of cyber, electronic warfare, information operations, deception, and denial to disrupt our command and control and thereby give the enemy an advantage in the decision cycle. By combining informationalized warfare with the accuracy and relative low cost of guided munitions, the victors on the next battlefield will fix and fracture their adversary with quick, decisive, and lethal effects across the entirety of the battlespace and immediately consolidate gains to make any military response politically unpalatable." (McCoy 2017, 2)

Therfore, the *"Multi-Domain Operations"* concept, as it was renamed in the Concept Version 2.0, requires truly integrated, resilient, and rapidly deployable military capabilities designed to achieve cross-domain maneuver and fires, capable of working together in a convergence that goes beyond synchronisation. (McCoy 2017, 3) Within the new vision, the core capabilities required to create an advantage in order to win the future fight should respond to one or multiple critical tasks, like competition, convergence, resilience, and force posture.

.

2. Mr. Senge's Model for Future Warfare

Being a guiding vision, the new concept has the possibility to resolve both today's operational environment and tomorrow's vision. As previously mentioned, it is developed to fulfil three core tasks - competition and the conflict continuum, compression, convergence, and expansion of the operating environment, as well as the future Force Components -, which represents, in fact, the foundation of the future of warfare for the US military.

The idea of competition seems to be perceived today by the conflict continuum (JP 3-0 Joint Operations 2018, 31), which represents the span of possibilities between peace and war, requiring American forces to be proficient across the full range of military operations „In short, the concept looks at competition as a period outside of open conflict; it is a contest over national interests with an adversary that exists short of conflict. To compete (and prevail), you must directly link your capability of waging all-out war with what you do in competition. As the concept states, this is not a new idea. Others might observe that it's no different than what we do today. But while we saythat our activities – from shaping to dominating to enabling - are connected, in practice, they too often are not. We must evolve the models we use to plan and execute operations if we want to remain competitive in the twenty-first century." (McCoy 2018, 3).

Unfortunatelly, the mental models described by the American scientist Peter M. Senge in his book[1] *„The Fifth Discipline: The Art & Practice of The Learning Organization"* do not represent a strong point for the US Army, even if the conflict continuum and phasing constructs are idealistic mental models for commanders, planners and decision-makers. This is because mental models are not solutions in themselves, but they give planners a way of phasing the military major operations. (Senge 2006, 187-188) The US Army's continuum conflict mental model is defined by competition short of conflict, conflict itself, and the return to competition. Gen. David Perkins, a former commander of the US Army's Training and Doctrine

[1] N.A.: Mental models are defined as deeply ingrained assumptions, generalizations, or even pictures or images that influence how we understand the world and how we take action.

Command, broadened the aperture of competition to a strategic perspective in a "Military Review" article as: "There is and always will be strategic competition. You are either winning or losing, present tense. Seldom will conflict result in a permanent win or loss. The linear depiction of peace to war and back again must be revised to reflect the cyclical nature of war where there are only positions of relative advantage." (Perkins, 2017). According to this mental model, there is not such thing as peace, but only competition and conflict. When settleing for peace, one might loose sight of how world is evolving and immediately place him/her at a disadvantage.

If mental models, like the conflict continuum and phasing construct, help define and organise problems and create possible solutions, the ones used in Afghanistan and Iraq to guide policy-makers, commanders and planners seems to be inadequate and misinterpreted by their costommers. This is why, the general perception is that the US Army needs revised models to give it the ability to stay competitive in a constantly changing environment.

In order to build up new mental models the US military thinkers should understand that the conflict continuum is not relational, but cyclic, in which military and non-military actions impact one another sequentially and simultaneously without a clear timeframe. These impacts change the environment and force competitors to control the operational tempo of the cycle, if they want to remain competitive. It also requires a change in how military operations will be modelled in the future.

A new mental model, focusing on the problem of competition confined by specifying time and space, provides an option outside of systematic build up of forces in shaping operations. In this new model, strategic plans should no longer be about steady-state shaping operation, but about winning in the competition period. Contingency plans should no longer be about setting the theater, but applying the ground work to effectively deter armed conflict, and if necessary, defeat adversaries if and when conflict arises. (Ionita 2021, 15)

Therefore, it is imperative necessary to build up a future menthal model to solve both the competition and conflict. Thir model should incorporate shaping considerations of future operating environment, as well as capability development to design new possible forces for dettering any possible adversary and providing resilience at home.

3. Multi-Domain New Challenges and Oportunities

After the North Atlantic Treaty Organisation (NATO) decided, in 2020, to include two new domains of operations in its Comprehensive Framework for Allied Operations – space and cyber -, more member states have started to think about and develop the US Army *"Multi-Domain Operations"* concept. In order to bring the concept at the strategic level, British military thinkers have transformed it into the *"Multi-Domain Integration (MDI)"* one, considering that the new approach will change the way British Forces operate and war fight, and the way capability are developed. According to the UK *"Integrated Operating Concept 2025"*, the UK Development, Concept and Doctrine Centre (DCDC) issued, in November 2020, the *"Joint Concept Note 1/20 Multi-Domain Integration"*, in which MDI is presented as „the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare." (Joint Concept Note 1/20 Multi-Domain Integration 2020, 3).

The aim of implementing this concept is to better compete with potential adversaries in this era of persistent competition, by conducting wars in a way that generates advantage through being better integrated across the three levels of warfare and all five operational domains: maritime, land, air, space, and cyber. (Joint Concept Note 1/20 Multi-Domain Integration 2020, 12)

The Western military thinkers already consider that the potential adversaries use different types of actions to achieve their objectives bellow the so-called war – *"political warfare"*, *"hybrid war"*, *"information superiority"*, *"new-type war"* or *"multi-sphere operations (mnogosfernoy operatsii)"* –, interoperating military and non-military capabilities with freedom acress to domains, both home and away, as well as using their gained experience in exploiting cyber, electromagnetic and information advanced technologies. Sophisticated operations that target systems are combined with more conventional military ones, like proxies, coercion, offensive cyber and lawfare, to disrupt Western systems in the early stages of any conflict and turn shaping operations into decisive ones.

The new threats pose by potential adversaries are exacerbated by technological advancement, precision effects, bluerred boundaries and time compression, which also represent drivers for change. This is why, the Western response is through multi-domain integration, because it seems that joint is no longer enough. As the JCN 1/20 stipulates, "MDI is about designing and configuring the Whole Force for dynamic and continuous integration of all global capabilities together, inside and outside the theatre, munitions and non-munitions, above and below the threshold of armed conflict. The greatest effect will be from drawing in as many capabilities as possible to apply combinations the adversary does not expect or cannot guard against. Forcing the enemy to defend all domains all the time from all directions will impose multiple dilemmas and open up vulnerabilities. It is not just an offensive concept; the ideas and designs are as applicable in defence and in engaging for influence." (Joint Concept Note 1/20 Multi-Domain Integration 2020, 11)

According to JCN 1/20, the multi-domain integration model comprises four tenets: (Joint Concept Note 1/20 Multi-Domain Integration 2020, 25):

- information advantage – enabling and effecting orchestration through comprehensive and persistent sensing and understanding of environments and audiences, which must be common across government and with allies;
- strategically postured – the global, domain-centric arrangement of capabilities;
- configured for the environments – readiness for multi-domain activity in operating areas and environments to influence the behaviour of selected audiences;
- creating and exploiting synergy – generating, timing and exploiting windows of opportunity for relative advantage by creating synergy.

In the current proposed model of MDI, there are a lot of challenges and opportunities. For example, the sense, understand, orchestrate functions are enabled and expressed just thorugh a Command, Control, Communications, Computers, Information, Surveillance and Target Acquisition (C_4ISTAR) system, which is an agile command and control capability, augmented by autonomy and automation. Moreover, the respective system will require technical, procedural, cultural and educational leaps to become a force multiplier.

Strategic posturing means to deploy right military capabilties in right places and integrate them with non-militry ones and Allies/Partners, where the operational level will interate strategically controlled multi-domain capabilties (like space and offensive cyber) with tactical ones. In a dynamic MDI, Component Command structures might not be the ultimate solution.

Tempo should be calibrated to be optimal in order to create windows of opportunities for exploiting the cross-domain synergy. There are identified or engineered within the combination of human, physical and information sub-environments according to relative domain strengths.

Still, the *"Multi-Domain Operations"* concept requires close reading and reflection to holistically address the complexity of future operating environment with considerable depth. For the respective concept to serve as a guiding vision for future conflicts it has to successfully incorporate technological advancements and diffusion, effectively leverage weaponised information, and efficiently address potential adversaries' disruptive political aims designed to upend the current international order.

Moreover, as the potential adversaries have already developed high-tech integrated systems, based on automation, machine learning, and Artificial Intelligence with the intent of using them in future conflicts, *the "Muti-Domain Operations"* concept has the main aim to go beyond present stove-piped and federated systems and programmes of record, in which cross-domain maneuver and fires require human solutions. It has to design new solutions for manned-unmanned teaming in the future.

* * *

The new concept of *"Multi-Domain Operations"* for future conflicts, being under development, represents the military innovative response to future treaths and challenges. It incorporates existing high-tech products and looks for perspectives and opportunities regarding how to achieve strategic advantages against potential adversaries in a future major conflict. Its main difference from other concepts, like *"the Mosaic Warfare"*, is represented by the idea of who will be in lead inside the manned – unmanned teaming: the people or the machine.

The task organisation of forces and systems according to the specifics of the mission to be accomplished is not something new, as is the idea of using systems networks in conflict. What is truly new about this concept is the speed and complexity with which it can combine the package of available flexible forces with the reinforced Command-Control system with emerging technology, operations divided into action elements and Mission Command, in order to achieve a real framework of a future modern Maneuver Warfare, focused on information. The main goal is not to allow the opponent the necessary time to predict and understand what is going to happen. At the Pentagon, the aim is to create a new approach to SoS, which can be flexibly networked and quickly configured to ensure the ability to resilience of operators. That means the use of any system or unit that has those characteristic functions that allow them to combine with other elements to achieve a desired joint capability at the time and place as being chosen by commanders. As distinguished councelor Robert O. Work stated, *"The Army that will find the most appropriate combination of technology and operational concepts will probably be at the top."*

The implementation of the new technologies will decisively contribute to the Multi-Domain Operations approach, being focused on obtaining a decisional advantage over an opponent. Support for decision-making by AI platforms, unmanned and autonomous systems, enhanced passive sensors, smaller weapons, and electronic and cyber warfare capabilities could impose complexity and confusion on an opponent and allow for targeted attacks on key targets. Thus, the emergence of a possible strategic paradigm on the preparation and conduct of future operations will be focused on the decision.

So far, neither NATO nor Romania has moved to such an approach in the recently conducted Strategic Defense Review (SDR). Concerns about the use of advanced technologies and the development of Smart Military Bases are found in the scientific events of NATO and some developed Member States, at an early stage. Unfortunately, this will further deepen the technological gap between the US and the European side of the Alliance.

BIBLIOGRAPHY:

IONITA, Craisor-Constantin. 2021. *Multi-Domain Operations Versus the Mosaic Warfare. Future Conflicts's Dillema Between Multi-Domain Operations and the Mosaic Warfare*. Chisinau, LAP LAMBERT Academic Publishing.

Joint Concept Note 1/20: Multi-Domain Integration. 2020. London, UK Ministry of Defence, LCSLS Headquarters.

JP 3-0 Joint Operations. 2017. „Incorporating Change 1 on 22 October 2018." Joint Chiefs of Staff, January 17, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

MCCOY, Kelly. 2017. "The Road to Multi-Domain Battle: An Original Story", *Modern War Institute,* October 27, 2017. https://mwi.usma.edu/road-multi-domain-battle-origin-story/

MCCOY, Kelly. 2018. "Competition, Conflict, and Mental Models of War: Whay you Need to Know About Multi-Domain Battle." *Modern War Institute*, January 26, 2018. https://mwi.usma.edu/competition-conflict-mental-models-war-need-know-multi-domain-battle/

PERKINS, David G., General. 2017. „Multi-Domain Battle the Advent of Twenty-First Century War." *Military Review*, noiembrie - decembrie 2017. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/Multi-Domain-Battle-The-Advent-of-Twenty-First-Century-War/.

SENGE, Peter M. 2006. The Fifth Discipline: The Art & Practice of The Learning Organization, New York, Currency and Doubleday.

DOI: 10.53477/2668-6511-22-22

NEW CHALLENGES FOR A FUTURE STATE DEFENCE

Fabian BAXA, Ph.D.,
Colonel (Ret), Academic Fellow, University of Defence, Brno, Czech Republic.
E-mail: fabian.baxa@unob.cz

Mgr. Aleš TESAŘ,
PhD Candidate, Lt. Colonel, Research Fellow, University of Defence, Brno, Czech Republic.
E-mail: ales.tesar@unob.cz

Abstract*: There is an increasing number of non-state actors acting recently as well as present armed conflicts aside of state actors when non-state actors being endowed with more economic and "military" power than smaller states what enable them a broad spectrum of activities in all domains explored by human civilisation. Nowadays even an inner space belongs already to activities of non-state actors. Cyber space is an arena of these actors since the beginning of its exploitation. Putting together, it is necessary to expect a growing number of frictions among various state and non-state actors having their own interests in the same areas and time. These frictions may lead to conflicts, even armed conflicts being presented by other activities than engagement of traditional armed forces against property or interests of both, state or non-state actors with an aim to gain some advantage. Actions in an inner space or in a cyber space could be more serious than small scale armed conflict. These actions might be considered as simple criminal or terroristic acts or as casus belli, like consequences of the 11th September 2001 situation. Who is in charge of judging a nature of the offensive actions between two non-state actors? What state is authorised to declare "war against terrorism" (or criminality?) towards one or all belling parties, which are non-state actors? This situation can arise more questions and this article has an ambition to elaborate some of them to address new challenges in the field of future state defence.*

Keywords*: advanced technologies, armed conflict, commercial companies, international law, private security companies.*

Introduction

Global security arena is continuously developing environment and this permanent changes have their reflections in an international legal arrangement. Among the others, one of important dimensions of these changes are actors playing their roles in accordance with their missions, ways and means, which can differ from roles of other, more traditional actors, internationally recognised states.

This article has an ambition to present results of research focused on two groups of relatively new actors of international scene, which already play important roles and these roles are going to be even more important in close future. The international legal environment should adapt itself in order to formulate clear rules how to treat these new actors to keep rule of law in these changeable environment.

The first group of relative actors are *private military and private security companies* (PMCs and PSCs) that are more and more officially used within running armed conflicts trying

to influence a concrete conflict or even to act officially on behalf of an internationally recognised government. The second group of new actors are international or national *private, commercial companies*, which capabilities exceed those within majority of ordinary states. This fact is important from the security as well from military point of view. Therefore, it is only the matter of time when these capabilities would be used in future armed conflicts on behalf of a concrete state or directly in order to enforce interests of the concrete company.

Concerning the first group of actors, they have been already active in recent as well as present running operations and with a high probability it is necessary to calculate their participation in future operations worldwide. There is not only in growing spectrum of these actors but their range of capabilities is also enlarging. These actors are not active in the area of operations in general, their activities can be monitored even during an ordinary, day-by-day life.

The second group of actors, international or national private, commercial companies, have capabilities in a scientific research, industrial production, international trade and turnover higher than smaller states. The reality is that resources devoted by private sector to the science are higher than by states in general. Some of these companies have dominant position in global trade in specific areas, e.g. software, including operational systems for personal computers used almost everywhere. Other companies from this group are even capable to launch missiles with human crew to the space, the capability owned by couple of states only. Both groups of actors are also considered as potential actors of hybrid threats.

Actors from both groups already have an intent as well as capabilities to act in the international arena as states and this trend is more and more clear. It brings new situation to the international legal environment and new challenges for ordinary states and international organisations acting in security and defence areas.

This article analyses the actors in the present and expected security environment and indicates proposals how to deal with expecting problems mentioned in analytical part. The intention is to address this issue and, by mentioning and analysing several typical examples from the recent and present period, to indicate a possible solution, both national and international level. The goal of this article is not to present universal solution of described situation and briefly analysed circumstances but to name the problem. Therefore, there are more questions than answers.

1. Private military companies within the present security environment and related trends

As mentioned in previous parts the main effort is paid to two groups of relatively new actors at the international security arena. This chapter offers several typical examples from both groups with short findings.

The first group contents private, commercially based companies focused on military or security capabilities offered to other actors of international security scene like states or international/national companies to solve assigned tasks. The existence of this kind of companies is not new, throughout history there are many examples of using existing or ad hoc organised groups that hiring former soldiers for hidden missions without discovering customers. In recent European history there are more pieces of information regarding presence of "*furtuna soldiers*" at all sides of an armed conflict in Balkans – Serbian side, Croatian side as well as Bosnian/Muslim side.

Nowadays, the new thing is that there are groups acting openly, even officially on behalf of their customers, like private battalions fighting in South-Eastern Ukraine (UKR) (Holcomb 2016, 33-71) since 2014. It is possible to say that due to lack of regular forces prepared in an appropriate state of readiness a Ukrainian government required several battalions organised, equipped, trained, paid, and owned by national physical persons. UKR General Staff tried to

keep control over these units with some problems associated with misuse of power against inhabitants of troubled areas, using of inappropriate power like extensive rocket launchers fire against inhabited areas, etc. The UKR government proclaims these inhabited areas as inseparable parts of the UKR territory. The main problem of engaging these battalions became when some of these units openly disobeyed orders of the UKR General Staff and marched with their small weapons in protest against the decision of the Kiev government in order to enforce their requirements. Lessons learnt from this situation are that private units can change their opinion quite quickly what may cause a serious problem.

Another example of an engagement of PMC is presence of a Wagner group in Syria (Bahgat 2021) as well as in Mali (Schwikowski et al. 2021). This group has been invited by a local government to fight with rebels in the country. Actions of this PMC included also offensive actions and there are connected with misuse of the power of the group towards local civilians and even mutiny to death of captured persons. Officially, this PMC is not connected to any country, but the owner of this group is from an inner circle of the President Putin therefore it is not far to the verity the group may act as an unofficial tool of foreign policy of the Russian Federation (RF) (Katz et al. 2020). Similar arguments are possible to find also here (GlobalSecurity 2021). The aim of this effort might be to keep Russian influence in several parts of the world supporting the idea of RF as a real superpower. Another unofficial goal might also be to keep a capable combat unit for potential use in future.

The third illustration of the recent activities is an example of the size of PMCs is American presence in Afghanistan where more than one half of a total personnel (Miller 2010) were contractors hired by the US authorities to work in support of the American presence there. These contractors conducted a broad spectrum of supportive tasks, from protection of US and NATO military facilities and bodyguards of VIPs to jobs in logistics, communication and information systems (CIS). There is not information concerning the use of these employees for offensive actions. It seems that the USA has learned a lesson from the engagement of PMCs in Iraq where, due to lack of training, members of the Blackwater company opened fire during a traffic jam at one of the junctions in Iraq.

In accordance with general observation the humanitarian law or the law of an armed conflict there are only two groups of personnel officially acting in armed conflict, military personnel and freedom fighters. A status of employees of PMCs is not specified because they do not belong to these groups. In addition, they are not counted as supportive civilian personnel because they are hired to use weapons for fighting. Using a general explanation of the military personnel when adjective “military” is connected just to the state, private companies have not a status of the state, therefore they cannot recruit and hire military personnel, just civilian employees.

Concerning the use of weapons for civilian personnel there is a generally valid rule that they may use weapons for self-defence of for defence of an object entrusted to care. Within an ordinary state just military units and Police may use weapons for offensive actions and employees of PMCs are not any of them. Therefore, it is hardly possible to find a right legal argument for the use of PMCs as a military unit without blessing from a government. The use of offensive actions on behalf of a private company or under tasking of leaders of a private company might be considered as an illegal use of power.

At the end, the presence of employees with weapons during armed conflict is problematic directly for these employees when captured hence they are not military soldiers or freedom fighters and without strong support from the hiring state, they could be treated as armed criminals.

There is a several partial findings regarding PMCs and their use in recent and running operations. The first is that there is no guarantee to ensure covered or opened disobedience of

such company especially when this company consists of volunteers from several nations. The second is that PMCs can be used in both defensive and offensive actions, which might be problematic according to present rules. The status of their personnel within armed conflict is not clear enough and various countries may see it differently.

In a case of the PMC hired by a government of a foreign state to suppress rebels, that misused its power and tortured captured citizens of this state and other states on hiring state territory, two questions may occur:

– What is a share of responsibility of the hiring state regarding this misuse of power from the side of the hired PMC?

– Who is responsible for protection of civilians when the state administration is not strong enough or not willing to do that?

Naturally, the state should be responsible to protect its citizens anywhere in the world, but if the state measures are not sufficient that state should be considered as a failed state and appropriate international organisations might take over the role of that failed state.

PMCs are considered as one of groups of actors mentioned in hybrid threats and hybrid warfare (HT/HW) papers as a tool for overt and covert subversion actions against the targeted state. Weissmann with his seven dimensions of the hybrid threats and hybrid warfare (Weissmann 2021, 65-67) is one of authors, which are worth being stated.

The PMCs are considered as an instrument of the hybrid threat stated already in the previous US Army Hybrid Threat Force Structure Organization Guide (Headquarters Department of the Army 2015, 2-9-2-17), issued in 2015.

Activities of these organisations are organised at the edge of an open armed conflict and hidden grey zone as actions under threshold of a regular war.

In conclusion of this analytical part, it is possible to formulate following finding:

Although PMCs are entirely new group of actors, their behaviour has been considerably changed. Today they act more overtly even they act directly in armed conflicts, often on behalf of concrete governments as a part of regular, state-controlled armed forces. Their members might face situations like soldiers of regular armed forces, e.g. captivity, but their status is not fully recognised by the present legislative framework. On the other hand, their members very often have problems with loyalty and obedience as well as with compliance of rules of armed conflict.

2. Civilian commercial companies, the present security environment and related trends

The second group of new actors consists of international or national commercial companies with capabilities exceeding those of majority of states in general, and *in concreto*, their "military-like" capabilities may be larger and more powerful than those of small or medium-sized countries. The first example are private companies with a capability to produce, launch and operate space equipment for their purpose (Rauenzahn et al. 2020). Recently one of these companies presented successfully its ability to launch missiles with a human crew to the inner space.

States and other private companies may hire this capability to satisfy their needs and interests and, on the contrary, other states and private companies may see it as a threat to their interests. Within the space where present traffic is already of quite high intensity then might occur an incident where the private satellite may crash into other, state-owned apparatus, which that state may consider as vital for its interests. There is a first question coming from this situation:

- When the private commercial organisation registered on the territory of one nation would launched attack with a use of weapons on a state-owned object on the territory of other state would it be considered as an armed attack against the state?

NATO Allied Command for Transformation (ACT) released several editions of a paper named Strategic Foresight Analysis (SFA) (NATO Allied Command Transformation 2017, 27-

28), where a situation of state - non-state actors conflict as one of possible crisis in future is mentioned. Even today, it is possible to find some examples of frictions between states and their organisations with commercial companies and once these frictions could convert into a direct conflict or even into the conflict with use of armed violence, concretely weapons. Especially in a situation of a cyber-attack where a definition of a weapon and an armed violence becomes much broader than before.

There are commercial companies devoting more financial resources for scientific research than majority of states therefore in future is possible to expect that these companies will be leaders of a progress in technology. Due to this fact, these companies might have bigger desire to control larger portion of global resources than many of states. Hence, a literature of political science considers willing and means as two necessities to launch hostility.

A similar example could be seen in a position of producers of critical elements of all modern electronics, like microprocessors and memories as well as electronic parts for any larger systems or constructions using any CIS parts, with the Industry 4.0 is critically depended. It is possible to join problems with Covid-19 pandemics negatively influencing not only production but also worldwide transport on a daily basis.

In addition, more than 70% of personal computers (PCs) in the world runs on one common operational system and majority of these PCs use a common office software and are connected to internet using routers and other network parts produced by several commercial companies. In some authoritative regimes, these producers might be influenced to satisfy interests of their administrations. It means there is a growing potential to be not only monitored but also to be targeted directly or indirectly as objects of blackmailing or objects of a cyber-attacks. Simply said, when a concrete commercial company having feeling that its interest are not filled up sufficiently they might misuse its world monopoly to organise hidden or open attack against interests of users regardless they are state organisations, commercial companies or private users. These attacking organisations may also work under command of their government. These attacks might be originally thought as attacks under threshold of armed attacks but targeted states might regard them as *casus belli*. This approach was already declared in a communique from NATO Summit in Wales in 2014 (NATO 2014).

The situation described above induces next question:

- Are states responsible for activities of commercial subjects registered and based on their territory?

At common conditions, regulations for all commercial subjects' operation of the state territory are parts of concession given to these subjects and state authorities are empowered to monitor activities of these subjects and, when necessary, may enforce fulfilment of set up rules. Similarly, when the state allows activities of international commercial subjects registered abroad on its territory it would have to setup an appropriate legal framework. Breach of this framework will lead to a trial where the whole company and/or their managers might be prosecuted. Problem may occur when the commercial subject is registered in some tax-paradise country where the local government is not keen to lose any income and therefore this registered subject breaching rules in other countries is not brought to responsibility. The reason might be simple – the local government is not strong or willing enough to enforce any rules towards registered companies. This situation leads to the next question:

- Is the state of registration responsible for abroad activities of registered companies and what are ways to bring this state to responsibility?

A similar situation appeared in Afghanistan (AFG) with a terrorist organisation named Al Qaeda, which members committed attacks on the USA territory. The USA asked AFG government to release perpetrators to the justice and to close down Al Qaeda facilities on AFG territory. When AFG government refused the USA within their "war against terrorism" recognised this refusal as *casus belli*.

The contemporary international law recognises that a status of war is possible to declare only by a state to another state or states not to a private organisation and it is not important whether terrorist or criminal one in its nature.

Taking into account a fact that a commercial company has not the same status as states in the international scene, therefore a commercial organisation is not possible to be in hostility neither with the state nor with other private organisations. The reason is simple: just the state has a territory, the private organisation may be an owner of a concrete part of the territory of the state. This organisation can sell its territory to another commercial company, physical person or to the state but not to another state. All parts of territory owned by any private organisations belong to the concrete states.

Responsibility of the states for activities of commercial companies using their facilities on the territory of the concrete state has been already mentioned and this situation leads to the next two questions:

- What might these states expect when these companies negatively influence interests of other states?
- Will it be a sufficient and internationally acceptable *casus belli* justifying an armed attack on a facility of the company located on the territory of the other concrete state?

Nowadays, this kind of the attack would be considered as an armed attack against a state territory and it may lead to an armed conflict.

There is also a possibility of damaging activities of international commercial companies outside of the territory of their homeland, the territory where these companies have their general management and headquarters (HQ). These actors may have their facilities on territories of other states, even on the territory where their targets, objects of their negative influence, are located. Typical example is a network of computers-zombies remote controlled from the company located on the territory of completely different state. This network might be used against a vital object of the targeted state causing damages higher than a small-scale armed conflict. Besides the clear responsibility of originator of the attack in this case is questionable what is sharing of responsibility for consequences of the attack among owners and users of remote-controlled PCs and management of attacked objects. The owners of remote-controlled computers did not pay enough attention to protect their computers and managers of attacked objects did not devote enough effort to have their protective measures sufficient.

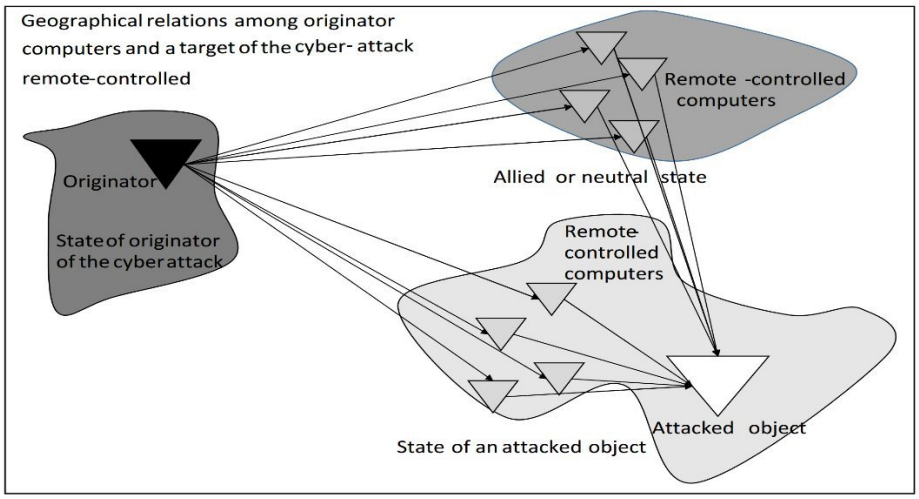

Figure no. 1: Example of territorial affiliation of an attacking organisation, used means and its targets

Using of weapons against a state organisation or a company registered on a territory of a concrete state or being important for this concrete state might be considered as a simple

criminal or perhaps as a terrorist act. This consideration is fully in responsibility of the concrete state, which territory or interest is targeted.

Considering the related situations also evokes a problem of terminology. When an armed conflict linked with the use of weapons is realised among non-state actors of the international arena treated as armed conflict or rather as a criminal or terrorist act? Similar problem with terminology comes from traditional definition of the weapons when the term weapon should include all means increasing human capabilities to limit interests of the opponent. In a case of cyber-attack should personal computers with their hardware and software used in cyber-attack be also treated as weapons with possible legal restrictions?

Similarly, as PMCs civilian commercial companies are also considered as a tool for economic pressure generation on the targeted state within the hybrid threat and hybrid warfare. Comparing to PMCs and their place in the fifth dimension mentioned by WEISSMANN´s paper (Weissmann 2021, 65-67), commercial companies are quoted as a part of the second economic dimension.

In conclusion of this analytical part of the article, it is possible to formulate following findings:

Although PMCs are entirely new group of actors, their behaviour has been considerably changed. Today they act more overtly even they act directly in armed conflicts, often on behalf of concrete governments as a part of regular, state-controlled armed forces. Their members might face situations like soldiers of regular armed forces, e.g. captivity, but their status is not fully recognised by the present legislative framework. On the other hand, their members very often have problems with loyalty and obedience as well as with compliance of rules of armed conflict.

Concluding this analytical part, it is possible to formulate this finding:

Commercial non-state actors like international companies are many times much stronger from both economic and security point of view and they play much more important role within the international arena. They have monopoly in hardware and software for CIS worldwide and they are more active even in inner space. It is a question of time when interests of these commercial companies will cross with interest of concrete states or other similar companies. In this case simple conflict of interests may turn to an armed conflict where some or all sides will use available capabilities. HQ and facilities of these companies are located on a territory of a concrete state, which might be different from states engaged in conflict but attack against objects on its territory might be considered as a *casus belli*. Moreover, dismantling of management of the commercial company or destruction of their facilities may plunge some states or some economic sector worldwide into economic crisis.

3. Possible ways to solve present and expected future challenges regarding new actors of the international security environment

Based on findings and structure of the previous chapter this part of the article pays attention to possible ways how to solve discovered problems. At the beginning it is suitable to categorise sides of conflict with a use of weapons. There are recognised three possibilities of sides of a conflict and these combinations are listed in the table no. 1.

Since it might be unclear whether the term *armed conflict* is linked only to relations among states or about factions inside the state, in the table is used wording *conflict with a use of weapons* when a commercial organisation is involved. The term *state* also includes state owned organisations. The use of terms *crime* or *conflict with a use of weapons* depends on an angle of view – the commercial company engaged itself in the conflict does not recognise this situation as a *crime* but its opponent may see it otherwise, unless that organization is element

of the armed forces (Protocol Additional to the Geneva Conventions of 12 August 1949, Art. 43) of a party involved in the armed conflict.

Table no. 1: Possible combinations of conflicts among the state and commercial organisations

1st actor	2nd and other actors	Characteristics of the conflict
state	state	armed conflict
state	commercial organisation	crime or conflict with a use of weapons
commercial organisation	commercial organisation	crime or conflict with a use of weapons

In the second table, there is an example of the possible list of groups of actors potentially acting against their objects of interests.

Table no. 2: Categories of actors

Categories of actors engaged in potential hostile/criminal acts against other their objects of interests
States
Economically powerful International or national company/society owning advanced technology
Private security/military companies owned by a private person and controlled by a government
Private security/military companies owned and controlled by a private person
Criminal individual or a criminal group

Table no. 3 contains information regarding categories of activities of above-mentioned actors.

Table no. 3: Categories of activities of actors

Aim of activity	Category
to enrich members of the company	(organised) national or international crime
to spread terror to support political, religious, or ideological goals	terrorist act or (organised) crime, depending on an angle of view
to damage property or interests to kill personnel of the concurrent company	(organised) national or international crime
to damage property or interests to kill personnel of the concurrent/opposing state	war, armed conflict (organised) national or international crime

It is quite clear that the state should be fully responsible for any activities of all subjects using its territory in a cause of weak administration or/and lack of willingness to enforce effective legislation. Even in this situation it is questionable if it is a case of *casus belli* from other states in their effort to protect their interests or interests of organisations registered at their territories including their citizens. They are other tools of national or international policy included in abbreviation DIME (Diplomatic, Information, Military, Economic) when military tools should be really last resort.

In assistance to the states, there are international security organisations and their role should be increased to become effective and active when necessary because the time when commercial organisations would have approach to capabilities to act globally is not a question of whether but when and how. These international organisations should be able to support member states in their effort to enforce more precise and strict rules towards international and

national commercial companies acting on their territory. This is the only way to avoid crisis originating from their territory and at the end becoming a target for measures from side of other states and international society.

The military as the most powerful tool of national as well as international policy are many times the first responder in operations where PMCs are deployed. Military leaders, HQ, staffs at all levels in a chain of command have to be prepared to act effectively in an environment where partners like PMCs may disobey given orders, might commit war crimes or to change the side in according to an intent of their warlords. Despite of these challenges military leaders have to be able to explore all possibilities not just avoid any contacts with the PMCs of uncertain origin because there is a threat that the opposite side of the armed conflict might be able to use even this fluid possibility for its profit.

In order to conclude this chapter, it is possible to formulate following findings:

- The most important measure how to limit conflicts with the use of weapons and armed power, is a strong and continuous supervision of companies having capabilities to launch armed attack to enforce their interests. It means the main role should play the states where these commercial companies are registered and/or where these companies conduct their activities. This responsibility of the concrete state should be supervised by appropriate international security organisations and these organisations should be empowered to take effective measures towards states as well as towards commercial companies. International legal environment should be improved accordingly. Within states, their legislation should be improved to enable them effective surveillance of companies acting on their territory while keeping necessary freedom of their commercial activities not aimed against other subjects.
- Similarly, it seems it is naive there will be no PMCs in future therefore it is necessary to improve appropriate national as well as international legal frameworks for their existence and activities. States, where these PMCs are registered as any other commercial companies, should be able to supervise their activities and activities of their owners because at the end the state is responsible for any illegal acts of companies registered at its territory including compensation of related damages.
- Concerning participation of regular armed forces within operations, where above mentioned actors are active, HQs, and staffs of an appropriate level in a chain of command should be prepared to cooperate with these actors when necessary while still keeping in mind their potential volatility and uncertain status of their members. Existing plans of operations, including Rules of Engagement (RoE), Standing Operating Procedures (SOPs), should be improved accordingly. Education and pre-deployment preparation of military personnel have to be changed as well.

Conclusions

International and even global security has many dimensions but one of them, physical security of human individuals, their families is the most important. Societies including states and their interests against external attacks have still a higher position in the scale of values. Human society for this purpose have built up a complex system of habits, written and not-written rules and legal acts at national and international levels. Therefore, it is always the sensitive matter when this system has appeared imperfect or insufficient due to the development of a situation and one of consequences of this development is the appearance of new actors. Especially when these new actors are in many times more capable than traditional states.

The aim of this article, declared as highlighting these new actors, their specifics and possible consequences of their activities, should be reached since sorting out all connected legal issues is far beyond this short paper. It is then understandable that questions mentioned here are

formulated but awaiting appropriate answers, which should be delivered after extensive work of experts on international as well as national law. The attention of these experts should be oriented at least to international law, especially humanitarian law and law of armed conflict.

Aside of questions for legal experts, information contained in this article could be used for education at advanced studies of security experts at international level to present them the whole complexity of security situation and to show them a holistic approach to local as well as global security challenges. At national level, the article tries to stress the importance of careful and precise formulation of legal aspects of duties and rights for all companies registered at national territory in order to avoid any international tension due to their activities abroad.

In military domain, this paper should be explored for preparation of higher echelons national and international HQ and staff members in order to formulate appropriate rules of engagement and other parts of plans of operations and related directives and orders.

Recognising an approach to the future called "known unknowns", generally we can expect even more actors having broader spectrum of interests as well as already known and even brand-new capabilities. Increasing number of actors will cause geometrically increasing number of their mutual interactions, which will be realised by new ways and means. Increasing number of interactions can probably lead to a number of conflicts and an ownership of capabilities to enforce their interests. When not paying enough attention to set up appropriate rules the unavoidable consequence of this situation is an increased probability of conflicts, even armed conflict between or better said among actors at international scene.

These challenges might be critical especially when existing and possible future technologies in wrong hands might cause serious international, even global problems, which this civilisation would not be able to solve. Complete cessation of all commercial activities in the field of security and defence or in advanced technology is not solution. In addition, hence initiative at any level leads this civilisation forward.

In this case a contemporary international legal system has faced in front of a complicated challenge hence it is necessary to define a role of PMCs and PSCs and legal positions of their employees during hostility in general, specifically in case of their rights in armed conflict in general and their status when captured. Similarly, it seems to be necessary to define a role of international society and its bodies in situations when international commercial companies are committing acts, which could be assessed as *casus belli* when they would be caused by states. Especially when their domestic states, states of their registration are not sufficiently strong to arrange rule of law.

At the very end, the final remark should be unfortunately that there are still more questions than clear, simple answers in this field.

BIBLIOGRAPHY:

BAHGAT, Farah. 2021. "Syria: NGOs file torture case against Russian Wagner fighters." *Deutsche Welle*, March 15, 2021. URL: https://www.dw.com/en/syria-ngos-file-torture-case-against-russian-wagner-fighters/a-56873162

GlobalSecurity. 2021. "Wagner Group: Private Military Company 'Wagner'." Last modified July 30, 2021. URL: https://www.globalsecurity.org/intell/world/russia/vagner.htm

Headquarters Department of the Army. 2015. Hybrid Threat Force Structure Organization Guide: TC 7-100.4. Washington, DC: Headquarters Department of the Army. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100x4.pdf

HOLCOMB, Franklin. 2016. The Order of Battle of the Ukrainian Armed Forces: A Key Component in European Security. Washington, DC: Institute for the Study of War. URL:

https://www.understandingwar.org/sites/default/files/ISW%20Ukrainian%20ORBAT%20Holcomb%202016_0.pdf

KATZ, Brian, SETH G. Jones, Catrina DOXSEE, and Nicholas HARRINGTON. 2020. "Moscow´s mercenary wars: The Expansion of Russian Private Military Companies." Center for Strategic and International Studies, September 2020. URL: https://russianpmcs.csis.org

MILLER, Christian T. 2010. "Industry Talk: Contractor Deaths Accelerating In Afghanistan As They Outnumber Soldiers." *Feral Jundi*, April 14, 2010. URL: http://feraljundi.com/1538/industry-talk-contractor-deaths-accelerating-in-afghanistan-as-they-outnumber-soldiers/

NATO Allied Command Transformation. 2017. Strategic Foresight Analysis: 2017 Report. Norfolk: Allied Command Transformation. URL: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf

NATO. 2014. "Wales Summit Declaration." September 5, 2014. Last modified August 30, 2018. URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.

RAUENZAHN, Brianna; WANG, Jasmine; CHUNG, Jamison; JACOBS, Peter; KAUFMAN, Aaron and PUGH, Hannah. 2020. "Regulating Commercial Space Activity." *The Regulatory Review*, June 6, 2020. URL: https://www.theregreview.org/2020/06/06/saturday-seminar-regulating-commercial-space-activity/

SCHWIKOWSKI, Martina, Mikhail BUSHUEV, Carole ASSIGNON, and Sandrine BLANCHARD. 2021. "Berlin and Paris concerned over Russian mercenaries in Mali." *Deutsche Welle*, September 16, 2021. URL: https://www.dw.com/en/berlin-and-paris-concerned-over-russian-mercenaries-in-mali/a-59201331

WEISSMANN, Mikael. 2021. "Conceptualizing and countering hybrid threats and hybrid warfare." *Hybrid Warfare*, edited by Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm, 61-82. London: Bloomsbury Publishing. URL: https://doi.org/10.5040/9781788317795.0011

DOI: 10.53477/2668-6511-22-23

WHY VALUES MATTER IN THE GLOBAL STRUGGLE FOR POWER. KEY IMPLICATIONS FOR EURO-ATLANTIC SECURITY

Cristina BOGZEANU, Ph.D.,
Senior Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania.
E-mail: bogzeanu.cristina@unap.ro

Abstract: *International environment becomes increasingly competitive and conflict prone. The present paper argues that political values subsumed to liberal democracy are an important component of the current global struggle for power and its purpose is to emphasize and argue the major importance of value-based cohesion for Euro-Atlantic actors, as well as the main challenges in this respect. In order to do so, the analysis is framed within the theories of power transition and security community as, together, they reflect both the manner in which values can act as a motivation for conflict and their function as a bond making the members of a security community able to pursue their interest in a conflicting international environment.*

Keywords*: power transition theory, security community, hybrid warfare, liberal democracy.*

1. Methodology

Brexit, US president conditioning compliance with collective security principles on financial aspects, EU member states infringing on fundamental EU values, EU leaders not agreeing on the manner in which the EU defence shall evolve, NATO member state deciding to cooperate with the Russian Federation in developing military equipment despite de worsening relations between Moscow and Western actors are all recent instances of the fragmentation of Euro-Atlantic cohesion. All these have been considered a sign of international liberalism failure (Mearsheimer 2019) (Wright 2018). At the same time, international security environment tends to become increasingly unstable: tensed relations between great powers, the on-going hybrid aggression, failure of armament control regimes, Russia's aggressive posture in Wider Black Sea Region, prolonged regional conflicts, recurrent waves of migration determined by conflict, the increasingly close perspective of a post-pandemic economic and financial crisis, the continuous rise of world military expenditures.

It is a world which seems to be increasingly governed by the principles of realism, of rational actors pursuing their interests defined in terms of power in an anarchic world. The thesis of this paper is that political liberalism is still of high importance not only in the current days, but also in the coming ones. This paper is based on the results of a previous research undertaken within the Centre for Defence and Security Studies, which revealed the need to deepen the analysis of the negative implications of the fragmentation of Euro-Atlantic cohesion (Centre for Defence and Security Strategic Studies 2021).

The argumentation is framed in the power transition theory and security communities as their theoretical assumptions illustrate the connection between defending shared values – cohesion of security communities – maintaining Euro-Atlantic actors' strategic relevance in the context of the sharpening geopolitical competition. Also, competition and conflict dynamics in international system is explained through power transition theory assumptions, emphasizing

that one of the main motivations of dissension is anchored in the ideological area. Thus, it is brought to the fore the need keeping our security community cohesive as here lies one of the main targets within hybrid aggression.

Negative trends of liberal democracy shall be illustrated with relevant studies and indexes and framed in the analysis of current events in the international arena. This paper concludes that, despite the increasing insecurity in the international system which determines the proclivity for a realist perspective on international relations, Euro-Atlantic actors need to watch and struggle for defending their values, namely liberal democratic values, as an essential pre-condition for them to be able to cope with the challenges arising from an increasingly competitive and conflict prone international system.

2. Specific of the current geopolitical competition

Power transition theory addresses both structural and dynamic aspects of international relations, starting from the premise that political interests are the source of all disputes among international actors (Tammen, et al. 2000, 6). Thus, it builds a theoretical framework useful in explaining the competition between great powers as it takes into account not only principles of realism (international actors are rational and their action in the international arena is determined by interests defined in terms of power), but also aspects that could rather be framed in the paradigm of idealism or constructivism, such as the fact that states sharing the same values are more likely to form enduring alliances and security communities. Thus, the theory can explain the international dynamics both from the perspective of increasing competitiveness and conflict between great powers, and from the perspective of cooperation within the Euro-Atlantic community.

Power transition theory premises that the resources of power at the international level are scarce and are concentrated at the level of few, thus creating the basis of a hierarchical vision on the international system. At the top of the hierarchy is a state that has the status of a dominant power (not a hegemon). It ensures its preponderance in terms of power over other actors by managing the international system according to a series of rules that respond to its own national aspirations and those of its allies (Tammen, et al. 2000, 6-7). Ronald L. Tammen et. all argue that conflicts arise at the international level when a great power (not the dominant one) becomes dissatisfied with its international status, and its ability to project influence beyond its own borders increases exponentially (Tammen, et al. 2000, 9-10). Dissatisfied powers seek to change the international *statu-quo* because they do not consider it to be in line with their long-term expectations and interests. The motivations invoked can be extremely diverse ranging from historical, cultural, territorial, ideological aspects (Tammen, et al. 2000, 9). In the current international context, one of the aspects that differentiate the *statu-quo* states, on the one hand, and the revisionist ones, on the other, is the type of government – democratic in the first case, authoritarian in the second. Therefore, conflict between great powers today also has a strong ideological motivation. Hybrid aggression targeting Euro-Atlantic community's vulnerabilities in this respect is illustrative in this line of thought.

The challenge of US status as primus inter pares has been achieved through economic and political instruments, both by Moscow and in Beijing, in distinct forms. Both of them are in conflict with Western actors, especially the United States – China, mainly on the economic ground, and Russia on the background of the actions in Wider Black Sea Region (WBSR), of manner of relating to the security regimes in Europe, but also of the hybrid aggression directed against the actors from the Euro-Atlantic security community. For the United States, China is the main strategic rival, tensions between the two escalating during D. Trump's presidential term. This conflict also infers on Europe, where China has interests and economic influence,

but also strengthens economic and political relations with states in the east or southeast of the continent, regions where not all countries are members of NATO and EU, but whose instability may affect the level of stability of European actors and, implicitly, the US. This is one of the reasons why, in EU's view, China is an "economic competitor in pursuit of technological leadership and a strategic rival that promotes alternative models of government" (European Commission and HR/VP 2019). The terms in which the EU refers to Beijing reflect the two dimensions of competition for power in this case – firstly, the economic one and, secondly, the political values-related one, as China takes opposite positions on the value system promoted and defended by the Euro-Atlantic community – liberal democracy[1]. It is, moreover, an area in which the official discourse of both sides tends towards inflexibility and even aggression, reflecting the dissatisfaction of Beijing with the international *statu-quo*.

At the same time, the actions of the Russian Federation have brought back the spectrum of military threat in Europe's security equation. Its central role in triggering and maintaining the Ukrainian crisis since 2014, aggressively pursuing its interests in WBSR and even in the Western Balkans, increasing military presence in WBSR, harnessing the "energy weapon" to promote regional interests, constantly opposing to the positions of Euro-Atlantic actors in managing regional crises, claiming new areas of interest (Arctic space) and even embarking on a race for space or for the prestige gained by medical resources (Sarcinschi, Competiția pentru vaccin și resurse medicale: o nouă fațetă a luptei pentru putere pe scena internațională 2020) are among the nuances that competition between the Russian Federation and the Euro-Atlantic community have known recently.

Russia's *divide et impera* strategy is one of the specific aspects of the conflicting relations with Western actors, a strategy also embraced by China recently. This is because one of the sources of power of the Euro-Atlantic community is the cohesion of NATO and the EU, but also because the Euro-Atlantic community already has a number of vulnerabilities in this direction, easily exploited by acts of hybrid aggression. Such actions are exemplified by interference in the electoral processes of EU and NATO member states and their neighbors, in particular by supporting extremist political formation (United States Senate 2018), constant, vehement and often aggressive contestation of the values promoted by them, etc. Thus, together with its military aggressiveness in European Eastern Neighbourhood, Russia's strategy has focused on contesting the values of liberal democracy (Barber, Foy and Barker 2019) and promoting ***apparently*** alternative values (traditional values, opposing to terrorism, neo-fascism, migration and the so-called "political correctness") (President of Russia 2013).

3. Political values as domain for great powers' competition and conflict

Also, power transition theory can provide a framework for explaining the relationship between international actors depending on the level of satisfaction with the *statu-quo* of the international system at a given time (Figure 1), thus providing a useful tool to assess the level of conflict potential between great power. When actors are satisfied and international rules are favourable to their own interests, they develop cooperative relationships, even going so far as to create *security communities*, *stable alliances* (NATO) or *economic integration organizations* (EU). We will consider the actors from the Euro-Atlantic space as exponents of an international state of affairs and of a set of rules that are challenged by the revisionist actors. China and the Russian Federation are considered the main resurgent powers, claiming the status of major world powers, as well as areas of strategic influence.

[1] See Beijing-Hong Kong relations, Taiwan relations, claiming sovereignty over areas of the South China Sea and the East China Sea, reaction to Western attempts to defend the rights of the Uighur minority (We Will Not Back Down under Sanctions, China warns the EU 2021).

Actors' view on world statu-quo **Nature of relations**	**Satisfied - Satisfied**	**Satisfied – Dissatisfied**	**Dissatisfied - Dissatisfied**
Cooperation  Non-cooperation	Security Community Economic Integration Confrontational competition	Competitive - improving Confrontational competition Hierarchical reordering war	Collusive partnership Escalating war

Figure 2: Joint Statu Quo Evaluation depending on the level of satisfaction in relation to the international status quo
Source: Ronald L. Tammen et al. all, 2000.

Joint *statu-quo* evaluation table explains the nature of the relations between actors depending on their degree of satisfaction with the current state of international system, with the rules governing the system in a given time. Satisfied actors, such as the US and its allies nowadays, establish relations of cooperation and build security communities and economic integration. NATO and EU picture the high institutionalization of this type of relation. In case of disagreement, satisfied actors verge towards confrontation competition. In our opinion, it is still another instance of cooperation within a security community, which is theoretically defined as "a transnational region, made up of sovereign states, whose populations maintain expectations based on peaceful change" (Adler and Barnett 1998, 30). Also, members resolve their conflicts other than by force, and is based on a number of shared values and meanings. Cooperation relations are set in various fields and its members have a number of common interests, usually anchored in the field of achieving a high degree of stability, security and prosperity. In other words, membership in a security community doesn't imply the absolute lack of conflict, but the approach of disagreement between members in ways other than confrontation.

Also relevant for the purpose of our paper is that these security communities know two forms of organization – "weakly connected", respectively "strongly connected" (Miroiu and Ungureanu 2006, 245). If the above definition applies to weakly connected security communities, a number of other features appear in the case of strongly connected communities. Thus, in order to have a strongly connected security community, it is necessary to meet the following conditions (Miroiu and Ungureanu 2006, 245-246):

a) sharing identities, values and meanings;

b) the actors that make it up develop direct relations in various fields;

c) is based on the mutual understanding of the interaction partners, which leads to the formulation of common interests, but also of mutual obligations.

Recent events reflect the fact that these characteristics, which form the basis of Euro-Atlantic cohesion, are today facing multiple challenges both inside and outside the community.

Joint *Statu-Quo* evaluation also explains the nature of the partnership between Russia and China in the context created after 2014, when Western actors imposed economic and diplomatic sanctions on Russia. Moscow-Beijing ties developed on these coordinates, thus limiting the effect of sanctions on Western actors, avoiding the situation of international isolation of Russia. The weight of this partnership increases if we consider that both are permanent members of the UN Security Council and both are in various forms in conflict with Western actors. This is why the partnership between the two countries has often been considered a "convenience" one (Ozawa 2019), meaning that they are open to cooperate when their interests converge, but without meeting the conditions for forming a security community. In this context, their interest in anchored on their aspiration of creating a multipolar world: "Both would like to see, and actively promote, the transition to a multipolar world with spheres of influence, one dominated by the US, China and Russia and where states, whether authoritarian or democratic, conduct their domestic and regional affairs independently of each other" (Ozawa 2019).

Thus, we may conclude that the current state of international system may be characterized through confrontational competition between *statu-quo* powers (US and its allies) and revisionist powers – China and Russia. Also, ideology, political values are one of the major domains where great power conflict happens. Ever since 2018, Freedom House warned that "the world's leading autocracies – Russia and China (...) are single-minded in their identification of democracy as a threat to their oppressive regimes, and they work relentlessly, with increasing sophistication, to undermine its institutions and cripple its principal advocates" (Abramowitz 2018). The same idea, but with reference to NATO, was resumed recently: "Political divergences within NATO are dangerous because they enable external actors, and in particular Russia and China, to exploit intra-Alliance differences and take advantage of individual Allies in ways that endanger their collective interests and security" (Reflection Group Appointed by the NATO Secretary General 2020, 16).

The current National Security Strategy of the Russian Federation states that the issue of moral leadership and the creation of an ideological basis for the future world order is becoming more urgent (Boyle 2021, 3). In China's strategic vision, strategic competition is presented not only in terms of rivalry between major powers, but also in the clash of different ideological systems (Office of the Secretary of Defence - China 2021, 1). Also, in NATO's terms, geopolitical competition supposes "the profusion and escalation of state-based rivalries and disputes over territory, resources, and *values*" (Reflection Group Appointed by the NATO Secretary General 2020, 16).

In this line of thought, we may conclude that political values are an area of disagreement between world's major powers. Also, as far as the Euro-Atlantic community is concerned, sharing the same vision on political values (in this case, liberal democracy) and laying them at the basis of their relations is key both in terms of security and stability and in terms of capacity of pursuing interests in a competitive global environment.

4. Liberal democracy trends to watch and reverse

The reason why this trend is a source of the most serious security threats is related to two major arguments:

- First of all, cohesion is the center of gravity of the Western power bloc, which has become a security community;
- Secondly, regardless of the level of analysis we are at, we identify challenges for this center of gravity of the Euro-Atlantic and European community, challenges that are mutually reinforcing.

For the US, strategic partnership with European actors and membership in NATO (even if it bears a large part of the Alliance's financial burden) is one of the major sources of power in relation to revisionist powers such as the Russian Federation and China. Moreover, the importance of belonging to a strategic bloc is also highlighted by the fact that the powers that are not satisfied with the international *statu quo* cooperate with each other when the aim is to weaken or counter the power of the Western bloc. In addition, for the European states, the construction and functioning of the EU has brought benefits not only in economic terms, but also the way in which small states, with limited resources of power, get to play a substantial role in the international arena by their membership to NATO and the EU.

The anchoring in the theoretical framework of the security community is relevant because it brings to the fore that these actors need cohesion in order to have the capacity to act in a relevant way on the international arena. As their solidarity and cohesion is based on sharing the same values of liberal democracy, we can refer to them as centre of gravity. In this regard, the implications of the theory of power transition for the stability of alliances and the formation of security communities are illustrative. Thus, the level of stability of alliances derives from the similarity of the interests of the state actors that compose them and from the common vision on the *statu quo* at international level, which is the basis of cooperative relations between them (Tammen, et al. 2000, 13). Both organizations have at their basis fundamental liberal democratic values[2].

This is the reason for which the decline of liberal democracy is one of the most serious challenges to be approached today as it is the source of major long-term threats to Euro-Atlantic security. At the beginning of 2020, Freedom House annual report warned about an unprecedented decline of democracy, emphasizing that the number of democracies is at its lowest in the last 25 years (Freedom House 2020). The conclusion of 2020 Democracy Index is similar goes in the same line (The Economist Intelligence Unit 2021), emphasizing that "only about half (49.4%) of the world's population live in a democracy of some sort, and even fewer (8.4%) reside in a "full democracy" (The Economist Intelligence Unit 2021, 3). Similarly, V-Dem report concludes that "the global decline during the past 10 years is steep and continues in 2020, especially in the Asia-Pacific region, Central Asia, Eastern Europe, and Latin America" (V-DEM 2021, 6). All these sources are showing the same trend of liberal democracy decline worldwide, a trend which has been amplified by the restrictive measures undertaken in the Covid-19 pandemic.

However, even on this background, Euro-Atlantic area is still the most democratic and safe one when compared to the rest of the world, there are two main peculiarities which we all shall consider warning signs. Firstly, there is the declining trend in terms of democratic quality and secondly, there is the net difference between Western Europe and North America, on the one hand, and, Eastern Europe, on the other, as the decline of liberal democracy in the latter is more steep (V-DEM 2021, 13). Hungary, Poland and Slovenia are experiencing the most substantial decline (V-DEM 2021, 18) (Freedom House 2021, 2). Thus, there arises a net risk of creating serious gaps within the Euro-Atlantic security community, difficult to manage and reduce as long as liberal democracy is on a declining trend[3].

[2] "They are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area" (NATO 1949); "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail" (The European Union 2010, 17).

[3] For extended examples and analyses in this respect, see: (Bogzeanu 2020b)

As mentioned before, the decline of democracies is not a recent trend, but it may have deeper implications under the impact of hybrid aggression. One of the peculiarities of hybrid aggression consists in the fact that, as far as Western states and societies are concerned, it doesn't not aim at occupying and controlling territories, but at disturbing their capacity to function properly (Lasconjarias 2017). Also, this type of aggression doesn't necessarily has in view to create new vulnerabilities, but to exploit and make the most of the ones already in place. In M. Galeotti's words, "a broad strategy of weakening the European Union and NATO, distancing Europe and the United States from each other, and generally creating a political and cultural environment more conducive for Moscow and its interests" (Galeotti 2017).

At the same time, the consistent history of this phenomenon, as well as the implications of various forms of hybrid aggression have made possible the development of a series of solutions at Euro-Atlantic level, opportunities to reduce threats and risks arising from the global tendency of becoming dominated by forms of government with undemocratic characteristics.

One of them is the concern for the development of the resilience of states and societies at NATO and EU level, with a focus on protecting democratic systems, as a solution for maintaining and strengthening cohesion at the level of the two organizations. Although, at first glance, it would have been expected that at the Alliance level, resilience would target governments' ability to function continuously, in crisis situations included, there is an initiative to set a *Centre of Excellence for Democratic Resilience*, which can be interpreted as a sign of the democratic values importance acknowledgement for the cohesion of the Alliance. The mission of this Centre would be to support allies, upon request, in strengthening the resilience of societies to withstand hostile actions coordinated by third parties on the proper functioning of democratic institutions and processes (Reflection Group Appointed by the NATO Secretary General 2020, 14).

Similarly, in the case of the EU the issue of the resilience of democracies goes beyond the text of the strategic documents (EU Global Strategy 2016), with many examples of measures taken in this direction. Among these, there are the introduction of a chapter dedicated to Cohesion, Resilience and Values in the Multiannual Financial Plan 2021-2027 (EU Council 2020) and the establishment of the Rule of Law Mechanism. Also in mid-2021, was adopted the European Democracy Action Plan (European Commission 2021), setting out specific measures to support the quality of democracy in European states in 3 major areas: elections free and fair, freedom of the press and misinformation.

Given the additional pressure on the degradation of the quality of democracy through direct and deliberate action, the development of a culture of security can be seen as part of efforts to strengthen the resilience of states and societies. In this sense, education in the spirit of developing the culture of security can create the basis for an informed report not only on the phenomena with security impact, but also on the skills and critical thinking necessary to discern the information to which we are exposed in each day.

Conclusions

In the current context of increasingly competitive international system, values, especially political ones, are used as motivation for conflict – main participants in the global struggle for power embrace different, even opposing values, praising the benefits of their own governance systems and considering the others flawed. This fact is also strongly supported by the conclusions of the studies on liberal democracy trends, acknowledging that the world is becoming less and less democratic and the states embracing autocracy or verging towards autocracy are more numerous with every year.

Also, there is a direct relation between shared political values (liberal democracy) - Euro-Atlantic security community cohesion (centre of gravity) – the ability to act cohesively

within the competitive and conflict prone international system. This centre of gravity which is currently flawed by internal forces and trends is under attack within the hybrid confrontation between the West and the revisionist powers.

Even though there are many claiming the end of the liberal world and transatlantic community, its resilience and the resilience of the two main organizations, proved throughout the years and various crises, shall not be underestimated. This even more as geopolitical competition between great powers may function as a possible stimulus for cohesion when confronted with a common threat.

BIBLIOGRAPHY:

ABRAMOWITZ, Michael J. *Freedom in the World 2018. Democracy in Crisis.* Freedom House, 2018.

ADLER, Emanuel, and BARNETT Michael. *Security Communities.* Cambridge, 1998.

BARBER, Lionel, FOY Henry, and BARKER Alex. "Vladimir Putin says liberalism has 'become obsolete'." *Financial Times*, 2019.

BOGZEANU, Cristina. "Rule of Law in the Context of the Double Blocking of 2021-2027 Multiannual Financial Framework and Next Generation EU." Edited by Centre for Defence and Security Strategic Studies. *Strategic Impact* ("Carol I" National Defence University) 77, no. 4 (2020b): 24-37.

BOYLE, Brendan. *Confronting Russia's Continuing Geopolitical and Ideological Challenge. Draft Report.* NATO Parliamentary Assembly, 2021.

Centre for Defence and Security Strategic Studies. *Riscuri și amenințări de securitate la adresa României.* Centre for Defence and Security Strategic Studies, „Carol I" National Defence University, Bucharest: "Carol" National Defence University Publishinghouse, 2021.

Comisia Europeană. "Rule of law mechanism." 2020.

EU Council. *Long-term EU budget 2021-2027 and recovery package.* 2020. https://www.consilium.europa.eu/en/policies/the-eu-budget/long-term-eu-budget-2021-2027/ (accessed 11 11, 2021).

EU Council. "Special meeting of the European Council (17, 18, 19, 20 and 21 July 2020) – Conclusions." Brussels, 2020.

EU Global Strategy. "A Global Strategy for the European Union's Foreign and Security Policy." 2016.

European Commission and HR/VP. "EU-China – A Strategic Outlook, 12 March 2019." 2019.

—. *European Democracy Action Plan.* 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2250 (accessed 11 11, 2021).

Freedom House. "Democracy Status." 2021.

Freedom House. "Democracy Status." 2020.

Freedom House. *Nations in Transit 2021. The antidemocratic turn.* Washington D.C.: Freedom House, 2021.

GALEOTTI, Mark. *Controlling Chaos: How Russia Manages its Political War in Europe.* European Council on Foreign Affairs, 2017.

LASCONJARIAS, Guillaume. *Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared.* NATO Defence College., 2017.

LINDBERG, Staffan I. "Autocratization Turns Viral. Democracy Report 202." V-Dem Institute, University of Gothenburg, March 2021.

MEARSHEIMER, John J. "Bound to Fail: The Rise and Fall of the Liberal International Order." *Internationa Security* 43, no. 4 (Spring 2019): 7-50.

MIROIU, Andrei, and Radu-Sebastian Ungureanu. *Manual de Relații Internaționale.* Iași: Polirom, 2006.

NATO 2030. "NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by NATO Secretary General." 2020.

NATO. "Commitment to enhance resilience issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw,." 2016.

NATO Strategic Communication Centre of Excellence. "NATO Strategic Communication Centre of Excellence." 2021.

NATO Strategic Concept. "Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon." 2010.

NATO. "The North Atlantic Treaty." 4 4, 1949. https://www.nato.int/cps/en/natohq/official_texts_17120.htm (accessed 11 11, 2021).

Office of the Secretary of Defence - China. "Military and Security Developments involving the People's Republic of China 2021. Annual Report to Congress." 2021, 1.

OZAWA, Mark. "Russia and China: 'axis of convenience' or 'stable strategic partnership'?"." NATO Defence College Policy Brief, No. 16, 2019.

President of Russia. *Vladimir Putin speech in the Meeting of the Valdai International Discussion Club.* 2013. http://en.kremlin.ru/events/president/news/19243.

Reflection Group Appointed by the NATO Secretary General. "NATO 2030: United for a New Era." NATO, 2020.

SARCINSCHI, Alexandra. „Competiția pentru vaccin și resurse medicale: o nouă fațetă a luptei pentru putere pe scena internațională." *Impact Strategic*, 2020: 7-23.

STARLING, Clementine G. "Trump's NATO Policy 'Trending Positive." *Atlantic Council* (Atlantic Council), 2018.

TAMMEN, Ronald L., et al. *Power Transitions: Strategies for the 21st Century.* Ronald L. Tammen, Jacek Kugler, Douglas Lemke, Allan C. Stamm III, Mark Abdollahian, Carole Alsharabati, A.F.K. Organski, New York: Chatham House Publishers, Seven Bridges Press, 2000.

The Economist Intelligence Unit. *Democracy Index 2020. In Sikness and In Health*>. 2021.

The European Centre of Excellence for Countering Hybrid Threats. "The European Centre of Excellence for Countering Hybrid Threats." 2021.

The European Union. *Consolidated Versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union.* Brussels, March 2010.

United States Senate. "Putin's Assymetric Assault on Democracy in Russia and Europe: Implications for US National Security. A Minority Staff Report Prepared for the Use of the Committee of Foreign Relations." 2018.

Uniunea Europeană. *Versiune Consolidată a Tratatului privind Uniunea Europeană și a Tratatului privind Funcționarea Uniunii Europene. Carta Drepturilor Fundamentale a Uniunii Europene.* Uniunea Europeană, Belgium: Oficiul pentru Publicații al Uniunii Europene, 2010.

V-DEM. *Autocratization Turns Viral. Democracy Report.* University of Gothenburg, 2021.

WRIGHT, Thomas. "The Return to Gret-Powern Rivalry was Inevitable." *The Atlantic*, 2018.

DOI: 10.53477/2668-6511-22-24

NUCLEAR GEOSTRATEGY OF THE POST-COLD WAR ERA

Marius-Cristian NEACȘU, Ph.D.,
Associate Professor, Bucharest University of Economic Studies, Romania.
E-mail: marius.neacsu@ase.ro

Silviu NEGUȚ, Ph.D.,
Professor, Bucharest University of Economic Studies, Romania.
E-mail: silviu.negut@gmail.com

Abstract: *The use of nuclear energy has changed the world's geopolitical and geostrategic landscape irreversibly, distinguishing another attribute of "high power", namely that of nuclear power, which not only means the possession of a nuclear arsenal, but also trade in civil nuclear technology (nuclear reactors for electricity generation) placing the selling state and the buyer in a geopolitical relationship. What's new? The emergence of a new nuclear military power, China, perceived as a "growing tiger", and new exporters of civil nuclear technology, Russia and China, which now concentrate 2/3 of reactor construction in the world after the long period of the Cold War when the global civilian nuclear energy market was dominated by the US.*

Keywords*: nuclear geopolitics; nuclear geostrategy; nuclear power; nuclear security.*

Introduction

Context. The Cold War was defined, among other things, at geostrategic level, by a genuine "nuclear balance", also referred to as "terror balance" in terms of international order, and we start from this perspective that nuclear technology possession places you in a select and very narrow club of "nuclear powers", it is also one of the most representative attributes of great power. The exclusivity came from the huge capacity to destroy possessed by nuclear bombs in military terms and from their potential for being used for persuasion and deterrence in negotiations.

The end of the Cold War changed the perspective of the ideological order, but it did not consist of the disappearance of nuclear arsenals or the temptation to threaten with their use.

As a result, the *aim* of this study is to identify the changes that have occurred in the distribution of nuclear power and the "balance", from a geopolitical and geostrategic point of view, after the end of the Cold War. The *emphasis of this research* is given by the fact that the military dimension of nuclear technology is not the only one that has geopolitical significance, but also the civil dimension, the latter becoming preeminent in the post-Cold War power games.

1. The geopolitical and geostrategic dimension of nuclear energy

The use of nuclear energy has irreversibly changed the world's geopolitical and geostrategic stage, distinguishing another attribute of "great power" or "superpower", namely that of *nuclear power*. And nuclear power does not mean only the possession of a nuclear arsenal, but also the commercialization of civil nuclear technology (nuclear reactors for electricity generation) placing the selling state and the buyer in a geopolitical relationship (Yoshida 2020, 12).

From this point of view, nuclear geostrategy has two dimensions:

a) military – the balance between nuclear powers (with their own arsenal, anti-missile shield, cyber and anti-satellite capabilities, etc.);

b) civil – the use of export of civil nuclear technology for geopolitical and geostrategic purposes.

In terms of the military dimension, the whole geopolitical equation of the Cold War was based on the *nuclear balance* (nuclear parity between the two superpowers, the US and the USSR), also known as the *terror balance* – the threat regarding the usage of nuclear weapons. The exact expression of the application of this balance on the ground, namely the perceived effects of the imbalance of the normal nuclear balance was the well-known "Cuban nuclear missile crisis" (1962), an episode we did not insist on (see Malița 2009, 382-403).

Additionally, the US is the only nuclear power that used the nuclear bomb in a real war (August 6th, 1945, launching the "Little boy" bomb in Hiroshima, and three days later on August 9th, "Fat Man" in Nagasaki – a nuclear attack that has led to the haste of the end of World War II, by taking Japan out of the game) and the first nuclear power to deliver civil nuclear technology and a market for peace-keeping since 1953 (The "Atoms for Peace" program).

As regards the military dimension, each US President has tried to change, to reform his predecessor's nuclear strategy, Paulsen (2014) summarizing all this doctrine development during the Cold War, as follows:

a) *the containment strategy* – specific to the starting point, when the United States were the planet's only nuclear power (1945-1953), initiated by President Harry Truman;

b) *the massive retaliation strategy* – was created during the Eisenhower administration, in the 50's, against the background of the emergence of the USSR as a nuclear player and the active conflicts in South Asia (Korean Peninsula); it was the period of the quantitative explosion, the US nuclear arsenal increasing from about 1,000 in 1953 to 18,000 nuclear warheads in 1960 (Paulsen 1994, 5);

c) *the flexible response strategy* depending on the context and situation – applied in the 60's ("Kennedy moment" and the mandate of Lyndon Johnson);

d) *the hard peace strategy*, a kind of peacekeeping through the manifestation of power (*peace through strenght*), applied in the 80's (the "Reagan era"), during which another geostrategic doctrine was initiated, namely the *Strategic Defence Initiative*, presented in literature under the term *"stars war"* (the design of anti-missile shields);

e) *the soft peace strategy*, i.e. peace through denuclearisation or peace through disarmaments, at the end of the 80's and early 90's in the Bush Sr. – Gorbaciov tandem.

Since the USSR entered the nuclear power club, the Soviets had only one dominant doctrine, namely the equivalence of US nuclear power through the quantitative increase in nuclear arsenal ("catch-up-to-the Americans", see Paulsen 1994, 16).

The 90's were a hesitating period in terms of international order (Cold Peace) and the manifestation of the American hegemony, following the implosion of the ideological and strategic adversary (the disappearance of the USSR as an actor and the geopolitical withdrawal of Moscow), have brought the individualization of another nuclear doctrine based on deterrence (*deterrence strategy*), during Clinton administration (for more details see Leveringhaus 2018, 77–90; Müller and Schaper 2004).

The geostrategic logic of the nuclear field in the present has not changed much compared to the one during the Cold War era (see also Hall, Capello and Lambert 1998), but there are some nuances that need to be mentioned:

Firstly, quantitatively, nuclear arsenal has been reduced, but the technological evolution (hypersonic missiles, cyber-attacks, missile shields, and so on) can influence the balance,

"altering" the classic Cold War model: "There are many more variables in the equation and future arms control negotiations will require the presence of the US, Russia, China to redesign the strategic stability" (Creedon et al. 2019, 4).

If, after the "missile crisis" in Cuba (1962), the United States, for example, had about it 30,000 nuclear warheads, in 2018, the total nuclear arsenal amounted to about 15,000 units, of which more than 90 % was held by Russia and the USA (6,850 and 6,550 units respectively), the rest being dispersed in France (2%, 300 units), followed by China (280 nuclear warheads), Great Britain (215), Pakistan (145), India (135), and between 1% and 2% each, less than one percentage being held by Israel (80 nuclear warheads) and North Korea with 15 nuclear warheads (*Ibidem*, 2). Close and somewhat more up-to-date values also provide other sources, with a relative decrease in US nuclear arsenal (5,550) and slight increases in China (350), Pakistan (165), India (156), North Korea, with uncertain values at the latter level, even three times higher, i.e. 40-50 (SIPRI 2021).

Secondly, the emergence of a new nuclear military power, China, is perceived as "a growing tiger – To expect China not to use its muscles is like waiting for a tiger's baby not to grow its teeth" (*Ibidem*, 6) – or as "the biggest player in the history of mankind" (Allison 2017, p. VII).

Thirdly, the emergence of new exporters of civil nuclear technology, Russia and China, which currently own 2/3 of reactor construction market around the world, after the global civil nuclear energy market was dominated by the US for a long time during the Cold War, with 41% of all reactors sold in the timeframe 1969-1990. After the end of the Cold War, between 1991 and 2017, it dropped to only 8% (Carless 2020, 19).

2. The "new" nuclear powers

Trade with nuclear materials and technologies is geopolitical by its nature (Nakano 2020, 3), each of the three first nuclear powers following another strategy:

a) the USA ("declining nuclear leader"), a *business* one;

b) Russia ("the new leader"), the largest supplier in the field (Szepers 2019, 1), a *geostrategic* one (Conca 2017); similar to the case of natural gas, the former Soviet-era Ministry of the Gas Industry became the state-owned Gazprom and the former Atomic Energy Ministry became Rosatom, both geostrategic instruments at the disposal of President Vladimir Putin, exporting technology for nuclear reactor construction in Belarus, India, Bangladesh, Turkey and Egypt;

c) China ("the next big leader"), a *geo-economics* one (increasing and expanding its economic power), building reactors in Pakistan, Uzbekistan, last together with Russia (Nakano 2020; de Blasio 2017, 15).

Therefore, at the moment, the US must share nuclear leadership with Russia and China, with the increase in competition over recent years being attributed to both Moscow and Beijing, both using trade in civil nuclear technology "to gain influence in regions of strategic value, especially Eastern Europe, South Asia and the Middle East" (Miller and Volpe 2018a). At least, in the last of the regions mentioned, Iran's nuclear ambitions have sparked a similar reaction from Saudi Arabia (Miller and Volpe 2018b, 27–46), with the kingdom under the US security umbrella becoming the target of the "geostrategic nuclear exports" (Hibbs 2017) of Russia and China.

In the same way, North Korea's unpredictability and aggressiveness regarding nuclear weapons – where nuclear power has this feature of being a tool almost exclusively used for the survival of the regime and also of the Kim dynasty (der Meer 2011), the frequency of the testing and the strength of the bombs being much higher during Kim Jong Un compared to his father

Kim Jong Il – could end up putting Japan in front of the same solution, namely to have its own nuclear arsenal (McMaster 2020).

While US and China are suppliers of globalization, both of which need a peace-based international order, the latter still preserving the rhetoric of the "second hit", which is "we will not strike first" – a defensive rhetoric, coupled, paradoxically, with an increase in offensive capacity in cyberspace and anti-satellite (Creedon et al. 2019, 6), Russia does not participate in globalization, judging and playing geostrategically well in conflictual situations. At the same time, Russia and China are perceived as "revisionist powers" (Rudolf 2020) – China, as a "systemic rival" from the point of view of the European Commission (*apud* Cline et al. 2020, 25), seeking to change the international order in their own interest and building spheres of influence. A complicated geostrategic equation...

3. Post-Cold War nuclear geostrategy elements

In the area of nuclear geostrategy, Herbert Raymond McMaster, former national Security Adviser (2017-2018) during the Trump administration, denounces the *"escalation control" doctrine* (McMaster 2020), initiated by Vladimir Putin to intimidate NATO member states and weaken Alliance cohesion: the threat of early nuclear attacks in Europe with the aim of putting the US in the face of a strategic dilemma, namely the risk of a nuclear holocaust or the negotiation of peace on Russia-favourable terms. Basically, a continuation of the principles of the "first hit" and the "tertiary part" during the Cold War.

The emergence of China as a nuclear power was analysed in some studies from the perspective of the Thucydides trap: "The rise of Athens and the fear it has established in Sparta have led to the inevitable war" (Allison 2017, VII), which, translated in terms of today's nuclear geostrategy, would sound like: "China's nuclear rise and fear caused in the US could make the inevitable war" (see also Gaub 2020), and the author highlighted some common features at former US President Donald Trump and Xi Jinping (Allison 2017, VII):

Both have been led by the common ambition to make each one of their nations "great again": if about the failure of Donald Trump as a "leader of the free world" we are already aware, as the announced doctrine is well-known, "let's make America great again", XI Jinping's achievement remains to be seen: China as a superpower; it is known only the Chinese time horizon, i.e. 2049 (the year when the *New Silk Road/Belt and Road Initiative* is also estimated to be finished), the year of Mao Zedong/Tsedun Centenary.

Identifying the other players as obstacles to their dreams: let's remember the mutual attacks on the virus subject in 2020, at the start of the COVID-19 pandemic, of the two protagonists (Donald Trump and XI Jinping) or Trump's roads in North Korea, in an attempt, which has not been successful, to make Kim Jong UN abandon the development of its nuclear capabilities (plus their hilarious rhetoric on the nuclear "button").

The pride/ego as a dominance of their *leadership* capabilities, which, at least from this perspective, can be similar to the strategic-nuclear confrontation in 1962, during the "Cuban missile crisis" between Nikita Hrusciov and J.F. Kennedy.

Also, both have taken a central role in revitalizing their own nations, using words as "radical change" on the domestic policy agenda and both were perceived as the exponents of nationalist-populist visions, each of which was clinging its own historical mission.

Joe Biden's coming to the White House meant a return to the nuclear geostrategy of the Obama administration, a series of words such as "no first use", "in last resort" or "extreme circumstances" defining the political framework regarding the use of nuclear weapons (Xiaobing 2021), which describe a nuclear geostrategy of a soft deterrence strategy, rather than a hard deterrence strategy.

The world is changing and the nuclear geostrategic equation is taking on as many variables as possible. For example, the United Arab Emirates is the first Arab state to operate a nuclear power plant (the Barakah nuclear power plant, currently unique in the whole Arab Peninsula, located close to the shore, in the south of the Persian Gulf, with 4 reactors already in operation, three in 2020 and the last one since 2021, with an installed capacity of 600 MW, covering 25% of national electricity consumption). And the United Arab Emirates have become the newest space actor, with the objective of achieving a human habitable colony on the planet Mars by 2117, a robotic space probe of its own, "Hope" ("Al-Amal"), already gravitating around the planet (arrived there on 9 February 2021).

Conclusions

The analysis of *nuclear geostrategy in the post-Cold War period* has led to a number of conclusions, as follows:

The cold War "cornerstone" was the nuclear balance. As one of the most relevant attributes of great power, nuclear weapon ownership had particular geostrategic significance during the Cold War, especially through the perspective of the strategic balance ("of terror", as it was called) which had to be maintained both in terms of quantity and quality of nuclear arsenal, and last but not least, through the number of nuclear powers in the world. The USSR's implosion and the end of the Cold War did not mean the disappearance of the nuclear threat or the disappearance of the nuclear weapons stocks owned by the great powers, but merely *the reconfiguration of nuclear geostrategy*.

In terms of nuclear geostrategy doctrines, of military origin, they have evolved from the offensive ones during the Cold War to the defensive ones of the present ("no first use"). Most of the American doctrines of the second half of the last century in the area of nuclear geostrategy were offensive, the *massive retaliation strategy* being just an example Currently, the *deterrence strategy* is the most used, which is true, has suffered a few nuances, from a "hard" version during the Trump administration to a "soft" one at present (which means, in fact, a return to the previous one during the Obama administration).

In the post-Cold War period, civil nuclear energy also took a geopolitical and geostrategic meanings. The possession of nuclear weapons, a characteristic of the Cold War, has been changed into a strategic field with the export of civil nuclear technology versus geopolitical dependence. There are two major exporters of civil nuclear technology at the moment, namely Russia and China, which together concentrate 2/3 of the reactor construction around the world, replacing the US as the dominant supplier in the field before the fall of the Berlin Wall.

The views of the current nuclear powers are different. While the US, as a civilian nuclear power, is perceived as a declining leader with a business vision, Russia is considered a "new leader", which uses the export of civil nuclear technology as a geopolitical and geostrategic tool, while the emerging Chinese has a geoeconomical strategy.

BIBLIOGRAPHY:

GRAHAM Allison. 2017. *Destined for War: Can America and China Escape Thucydides's Trap?* Boston/New York: Houghton Mifflin Harcourt.

BLASIO, Nicola de and Richard NEPHEW. 2017. *The Geopolitics of Nuclear Power and Technology.* New York: Center on Global Energy Policy, Columbia University. URL: https://energypolicy.columbia

edu/sites/default/files/The%20Geopolitics%20of%20Nuclear%20Power%20and%20Technology%20033017.pdf

CARLESS, Travis. 2020. "The US Shouldn't Abandon the Nuclear Energy Market." Science and Technology 36, no. 2 (Winter): 19–22. URL: https://issues.org/wp-content/uploads/2020/01/Carless-The-US-Shouldnt-Abandon-the-Nuclear-Energy-Market-Winter-2020.pdf

CLINE, Mary K., MCCAFFREY, RICKERT Courtney, LAWLESS, Kyle P. and BEHRENDT Sven. 2020. 2020 Geostrategic Outlook: Global rebalancing raises uncertainty for business. A transformative age in geopolitics. London: Ernst & Young Global Limited, Geostrategic Business Group. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/geostrategy/ey-gbg-2020-geostrategic-outlook.pdf?download

CONCA, James. 2017. "The Geopolitics of The Global Nuclear Landscape." Accessed October 8, 2021. URL: https://www.forbes.com/sites/jamesconca/2017/05/20/the-geopolitics-of-the-global-nuclear-landscape/?sh=69e227c75f68

CREEDON, Madelyn, EINHORN, Robert, JENKINS, Bonnie, MALONEY, Suzanne, O'HANLON, Michael, Pak, JUNG, Rose, FRANK and Strobe TALBOTT. 2019. "Managing Risk: Nuclear Weapons in the New Geopolitics." Interview by Bruce Jones. Foreign Policy, February 11, 2019. Transcript. URL: https://www.brookings.edu/wp-content/uploads/2019/02/FP_20190211_nonproliferation_interview.pdf

GAUB, Florence. 2020. Conflicts to come: 15 scenarios for 2030. Paris: European Union for Security Studies.

HALL, Gwendolyn M., CAPELLO, John T. and LAMBERT Stephen R. 1998. A Post-Cold War Nuclear Strategy Model. USAF Academy (Colorado): USAF Institute for National Security Studies. URL: https://www.hsdl.org/?view&did=437817

HIBBS, Mark. 2017. "Does the U.S. Nuclear Industry Have a Future?." Accessed October 8, 2021. URL: https://carnegieendowment.org/2017/08/10/does-u.s.-nuclear-industry-have-future-pub-72797

LEVERINGHAUS, Nicola. 2018. "Beyond 'hangovers': The new parameters of post–Cold War nuclear strategy." In New Directions in Strategic Thinking 2.0, edited by Russell W. Glenn, 77–90. Canberra: Australian National University Press.

MALIȚA, Mircea. 2009. "Criza rachetelor: ONU, New York, 1962." In Pagini din diplomația României, edited by Ion Anghel, Lucian Petrescu, Valeriu Tudor, 382–403. Iași: Editura Junimea.

MCMASTER, Herbert Raymond. 2020. Battlegrounds: The Fight to Defend the Free World. New York: HarperCollins.

MEER, Sico van der. 2011. "Geopolitics and Nuclear Weapons: North Korean Provocations as a Tool for Regime Survival." Studia Diplomatica LXIV, no. 3: 53–65.

MILLER, Nicholas and Tristan VOLPE. 2018b. "Abstinence or Tolerance: Managing Nuclear Ambitions in Saudi Arabia." The Washington Quarterly 41, no. 2: 27–46.

MILLER, Nicholas and VOLPE Tristan. 2018a. "Geostrategic Nuclear Exports: The Competition for Influence in Saudi Arabia." Accessed October 8, 2021. URL: https://warontherocks.com/2018/02/geostrategic-nuclear-exports-competition-influence-saudi-arabia/

MÜLLER, Harald and SCHAPER, Annette. 2004. US Nuclear Policy after the Cold War. Translated by Catherine Mulder. Frankfurt: Peace Research Institute.

NAKANO, Jane. 2020. The Changing Geopolitics of Nuclear Energy. A Look at the United States, Russia, and China. Washington D.C.: Center for Strategic & International Studies. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200416_Nakano_NuclearEnergy_UPDATED%20FINAL.pdf?heOTjmYgA_5HxCUbVIZ2PGedzzQNg24v

PAULSEN, Richard A. 1994. The role of US nuclear weapons in the post-Cold War era. Maxwell Air Force Base (Alabama, USA): Air University Press. URL: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/b_0058_paulsen_role_nuclear_weapons.pdf

RUDOLF, Peter. 2020. "U.S. Geopolitics and Nuclear Deterrence in the Era of Great Power Competitions." Political Science Quarterly 136, no. 1: 129–153. URL: https://doi.org/10.1002/polq.13132

SCHEPERS, Névine. 2019. "Russia's Nuclear Energy Exports: Status, Prospects and Implications." Non-Proliferation and Disarmament Papers, no. 61 (February): 1–14. URL: https://docs.google.com/viewerng/viewer?url=http://www.nonproliferation.eu/wp-content/uploads/2019/03/ EUNPDC_no-61_FINAL.pdf&hl=en

SIPRI. 2021. "Global nuclear arsenals grow as states continue to modernize–New SIPRI Yearbook out now." Accessed October 9, 2021. URL: https://sipri.org/media/press-release/2021/global-nuclear-arsenals-grow-states-continue-modernize-new-sipri-yearbook-out-now

XIAOBING, Guo. 2021. "Biden can push through 'no first use' nuclear policy if sincere." Accessed October 9, 2021. URL: https://www.globaltimes.cn/page/202107/1228579.shtml

YOSHIDA, Phyllis Genther. 2020. Japan's Nuclear Reactor Fleet: The Geopolitical and Climate Implications of Accelerated Decommissioning. Washington D.C.: Global Energy Center, Atlantic Council. URL: https://www.atlanticcouncil.org/wp-content/uploads/2020/12/AC_Japan_FINAL.pdf

DOI: 10.53477/2668-6511-22-25

UKRAINE – STUCK BETWEEN RUSSIA AND THE WEST

Lara-Teodora POPESCU,
Student, Faculty of Political Science of the University of Bucharest, Romania.
E-mail: lara.popescu@yahoo.com

Abstract*: For some time now, Ukraine has been internally divided between those who support Russia and those who fight for the westernization of the country through its affiliation with NATO and the EU. Both the European Neighbourhood Policy (ENP) – and later the Eastern Partnership (EaP) policy – as well as Russia's foreign policy, have been fuelling more and more this internal divide, with every strategy implemented by the EU in that direction leading to violent responses from Russia, which had very significant consequences on Ukraine. This paper aims to present, through qualitative analysis, the present geopolitical situation of Ukraine, which seems to be unable to move forward in a definitive direction. Throughout this essay I will analyse the events that led to the impasse in which Kyiv is stuck now, also touching upon the tense relation between the EU and Russia. Towards the end of the paper, further possible strategies and scenarios are suggested, considering and examining the tense situation in the whole Eastern Neighbourhood. Comparisons between other EaP states and Ukraine are also going to be presented in order to obtain a complete picture of the situation.*

Keywords: *Ukraine; Europe; the Eastern Partnership; Russia; NATO; the European Union; strategic forecasting; geopolitics.*

Introduction

Ever since it became an independent state in 1991, Ukraine has slowly, but steadily, detached itself from the influence of Russia and shifted towards the West. Ukraine's NATO accession has been negotiated since the 1990s, at the moment being a non-associated member of NATO and having participated in several military operations (Olech 2019). Russia has always had its reservations towards NATO, perceiving the organization as an instrument of the US for expanding its sphere of influence. Therefore, when not only NATO but also the EU through its Eastern Partnership (EaP) policy initiative started to implement closer cooperation with the Russian perceived "near abroad" states – but especially Ukraine – Russia felt both humiliated and threatened (Sauer 2017). Since the inauguration of the Eastern Partnership (EaP) in 2009, the EU integration of the Eastern Neighbourhood states has been in continuous development. This has raised some severe issues for Russia, as the objectives of the policy initiative directly clash with Moscow's interests. Russia has always been sensitive when it comes to the post-Soviet states, as it perceives their cultures to be deeply interconnected, considering the history they share. Thus, it did not come as a surprise when Russia publicly expressed its opposition to the EaP, NATO, or any other Western affiliation of its "near abroad". At the moment of writing, the situation is probably the tensest it has ever been since the Cold War, and not only for Russia and the European Union. The EaP states also find themselves in an impasse. If they choose to have deeper forms of integration with the EU and thus break away from Russia's influence, then not only the support previously offered by Russia is going to be challenged, but also the assurance of peaceful coexistence (Delcour 2018). The crisis in Ukraine exemplifies in the best possible way how the 'peaceful coexistence' can be significantly threatened when Russia feels that its sphere of influence is being jeopardized. Thus, by

analysing the case of Ukraine, which can be argued that represents a 'soft spot' for Russia, predictions about the relation between Russia and the EU can be made, especially in what concerns the policies directed towards the EaP states.

1. The Ukrainian Crisis and its implications

From Russia's perspective, the European Union's involvement in the post-Soviet space does not only present great obstacles for further Russian integration of the former Soviet Republics but is also a direct threat to the Russian security and status in the international arena. On the one hand, economic integration with the near abroad states represents an essential objective for Russia, which has been hindered by those states' interest in tying closer relations with the EU. Until recently, the EaP states were greatly dependent on Russia, thus contributing heavily to Moscow's economy. However, in the past years, the dependency on Russia has been drastically decreasing as a result of the deeper EU integration. This has been a great concern for Russia, especially in the case of Ukraine, Georgia and Moldova, which each signed an EU Association Agreement that incorporates a Deep and Comprehensive Free Trade Area (DCFTA). Through the signing of the DCFTAs instead of adhering to the Eurasian Economic Union, the three eastern nations clearly stated their choice for the EU to the detriment of Russia (Koeth 2014). This further increased the tensions between Russia and the EU, as the three states are very important trade partners for Russia, in particular Ukraine, which is still Moscow's main trading partner from the region, even though the crisis of 2014 has halted the growth of both imports and exports between the two (Socoliuc and Maha 2019).

Throughout 2013 and 2014, major protests supporting Ukraine's cooperation with the EU took place all over the country as a result of President Yanukovych's decision to suspend the signing of a political and economic association agreement with the EU to the detriment of a financial and economic package coming from Russia. The protests ended with Yanukovych's resignation, the unfolding of the events coming as a complete shock for Russia. Feeling threatened by the sudden change of heart of the Ukrainian population, as Moscow perceived it, Putin reacted immediately and put into action a plan that would prevent Ukraine from joining NATO – the annexation of Crimea (Trenin 2014).

Even though Russia's fault in this crisis is obvious and cannot be denied by anyone, many scholars were quick to acknowledge the West's negligence too, or at least its inability to foresee the risks that their actions bore. The literature has heavily debated NATO's decision to invite Ukraine into the organization, as Russia has repeatedly stated, ever since the 1990s, that it would react in the case of Ukraine joining a western alliance such as NATO or the EU. Thus, the West could not have been that oblivious to not realize the most probable consequences of its actions. The only explanation found to rationalize the alliance's decision lies in its naïve faith in the evolving liberal world order which implies worldwide peace and mutual understanding. However, this argument is severely flawed because, even though it explains NATO's enlargement to the East, it does not justify the exclusion of Russia from this 'perceived East' (Sauer 2017). Moreover, it partially explains Russia's distrust of the 'military' nature of the organization. Considering Moscow's point of view, as its borders were threatened by stationing Western troops, it is legitimate to say that Russia's hostile actions were not driven exclusively by an imperialist desire to take back its sphere of influence (Mearsheimer 2014).

Especially in the case of Ukraine, Russia perceives NATO as a military extension of the EU. The cases in which NATO has served the interests of the EU under the condition of safeguarding the independence and territorial integrity of EU member states and its allies has led Russia to be more and more suspicious of the association between the two actors. In its view, the plans of the EU and NATO are deeply interconnected, with the accession of Ukraine to NATO automatically leading to further integration with the EU and vice versa. Therefore,

Russia's hostility towards Ukraine is explained by the support it received from the West. After the 2014 events, both NATO and the EU imposed significant sanctions on Russia, showing their uncontested sympathy for Ukraine. What is interesting to point out is that the EU member states agreed to a stern common response to the crisis in Ukraine. This came as a surprise for the whole world, as the EU is known for being quite divided when it comes to its foreign policies, especially on a subject on which its member states' interests greatly varied. Some member states (as Italy, Greece and Hungary) were heavily economically dependent on Russia, making them more reserved to a harsh response. However, the common decision to support Ukraine was based rather on the perceived European norms of sovereignty and self-determination than on the member states' interests, as Russia's intervention was unanimously considered "a fundamental breach of the Ukrainians' right to self-determination" (Sjursen and Rosén 2017). This common decision of the EU showed the gravity of the problem, as it was perceived from a Western liberal perspective, especially as the member states rarely agree to a common approach to foreign affairs. In this case, they found it completely necessary to show a united front in condemning Russia for its actions and supporting Ukraine in tackling this crisis. Considering that the Western powers continued to show even greater support for Ukraine after Russia's annexation of Crimea, one can conclude that Ukraine finds itself in a paradoxical situation. On the one hand, Russia is still extremely sensitive to the Western assistance that Ukraine has been increasingly receiving, thus maintaining a tense relation with Kyiv through its support for the separatist groups in Eastern and Southern Ukraine. On the other hand, Ukraine is not yet ready to detach itself completely from Russia and join the West, as it is still dependent on Moscow, at least from an economic perspective.

2. The path towards "Europeanization"

Bringing Ukraine closer to the EU, thus drastically undermining the influence that Russia still has over the country, is not essential merely for economic and ideological reasons. Security also represents a great part of the EU's interest in Ukraine, especially if we consider the theory that the EU adopted an imperialist geopolitical model in the creation of the ENP, which further merged with various geopolitical strategies. In this sense, the EU aims to create a security buffer zone, which aims to soften the external borders with the immediate neighbours, more specifically the ENP countries (Browning and Joenniemi 2008). In this case, Ukraine is of great geostrategic importance for the EU, especially for its Baltic member states, as any aggression happening in Ukraine would rapidly escalate the concerns about the Baltic states' own security. This was the case with the 2014 Crimean crisis when the peninsula was annexed by the Russian Federation and the three Baltic states (Estonia, Latvia, and Lithuania) put significant pressure on the EU to implement policies that would create closer partnerships with Ukraine, thus leading to the EaP (Vilson 2017).

Even though the EaP implies that Ukraine should adopt the EU acquis communautaire, the process is significantly more complex in a country severely influenced by the personal interests of the Ukrainian political elites and powerful local groups. Ukraine's reforms are usually disrupted by its oligarchy, as it mostly controls the process of decision-making through the leverage it has on the corrupt Ukrainian political class (Wilson 2016). The democratic reforms that are being pushed by the EU on Ukraine's institutional framework, but especially on its judicial system, are either reinterpreted or directly blocked by the richest people in Ukraine if their interests are not fulfilled by EU law (Terzyan 2020). Many scholars (Wilson 2016; Terzyan 2020; Åslund 2014) argue that the only solution to improve Ukraine's responsiveness towards the EU policies is to deoligarchize the system, thus separating and balancing the executive, legislative and judiciary powers. However, I believe that

deoligarchization is very unlikely to take place in Ukraine, thus being munch easier to cut the ties between the political elites and the oligarchs. This process would be dependent on anticorruption work within the state but is much more accessible than reframing the economic legislation of the country. Furthermore, the push for international partnerships, especially opening the market for international trade outside of Russia's sphere of influence, is argued that might promote a change in the oligarchs' perception of formal, democratic institutions (Melnykovska and Schweickert 2008).

3. The "Worst Case Scenario"

Ukraine is of great geostrategic importance for both Russia and the EU, as it can serve as a buffer zone for both actors. The clashing interests in Ukraine can be easily explained by geopolitics, as great powers do not respond well to potential threats close to their borders (Mearsheimer 2014). Furthermore, Russia is still the main trading partner of Ukraine, mainly because it is still dependent on the Russian refined petroleum. Ukraine has spent 6,62 billion dollars on imports coming from Russia alone in 2019 (OEC 2021). Therefore, Russia's fears are not limited to its security dimension, the prospect of Ukraine integrating with the West having great economic repercussions for Moscow too. At the same time, Ukraine is very important from this point of view to the EU too. Ukraine represents the main trading partner of the EU out of the EaP states (WITS 2021), thus occupying an even more important role to Brussels than Belarus and Moldova (Socoliuc and Maha 2019). Once again, Ukraine finds itself between the EU and Russia from an economic perspective too. If Kyiv continues on the same indecisive path, being unable to choose a side and continuing alternating between the two actors, it could end in a military altercation between Russia and the West. Ukraine has been constantly fuelling the tensions between the two sides, driving them to act recklessly, without considering the strategic long-term consequences. Therefore, the lack of cooperation between the West and Russia, particularly concerning the situation of Ukraine, could lead to the nation becoming a literal fighting front.

This scenario could be possible especially if one considers Russia's view of its status as a great power being undermined by the West. Ever since President Putin's Munich speech, Russia has repeatedly stated its dissatisfaction with the decision-making process in Europe, as it feels left out of major decisions that have consequences for the whole European continent, Russia included. Moscow drastically opposes the role of the leader undertaken by the West in Europe through both the EU and NATO. In 2007, Putin argued that the only actor that should have the authority to use military power is the UN, as the organization does not have a leading state that takes all the important decisions, in contrast to the EU and NATO (Pacer 2016). In this sense, Russia still perceives the world as bipolar, with the West being fully controlled by the US. According to Putin, both NATO and the EU are just instruments of propagating American views and interests overseas. Nevertheless, the EU has evolved significantly since the end of the Cold War, being able to assure its members' economic and political safety without the support of the US for a long time now. Over the past few years, Russia has been trying to challenge the liberal international order created by the West at several levels (diplomatic, political and security) through its approaches in foreign policy, doubting the motives behind every action taken by the West in Moscow's sphere of influence (Kanet 2018). However, even if Russia hunts for every chance to contest the liberal international order, the reality is that the liberal values are so deeply rooted all around the world that even Moscow is dependent on them to a certain degree (Ikenberry 2018).

4. Policy Recommendations

The EU should treat the neighbouring countries differently than its potential members, especially as membership is out of the discussion for the EaP states. As the EaP's institutional design is inspired by the EU enlargement process, Ukraine, Moldova and Georgia can find themselves overwhelmed by the EU's demands, as their biggest goal (membership in the EU) is off the table. The EU should personalize its approach particularly for each of these countries, as their pace of development is not that similar. A 'one size fits all' concept might be very problematic, especially as the three countries have a strong record of democratic instability that is still fuelled, up to a certain degree, by Russia. Thus, the EU should not force its norms and values through the complete implementation of the European acquis on countries that are still heavily influenced by Russia. In the case of Ukraine, the internal division between those who support the EU and those who side with Russia made it clear that the full implementation of the European acquis can be too heavy on the present state of the country. Considering Russia's contestation of the international liberal order, the implementation of common European values by the Eastern Partnership countries – especially Ukraine – can be seen by Russia as a direct threat to its security and influence in the post-Soviet space.

Integrating Russia in its Eastern Partnership would be unacceptable for Moscow as it would not tolerate the same treatment the other near abroad states enjoy. However, the EU should treat Russia as their 'neighbour', meaning that it should handle Moscow as one of its partner nations. The EU should work together with the Russian Federation to achieve a compatible identity that would suit both parties, without negating either one's core values. The treatment of Russia should be indeed different from the other EaP states' treatment, but it should not emphasize Russia's 'normative otherness' (Delcour, 2018), thus not leaving any space for wrongful interpretation. Through these measures that would support proper cooperation between the two great powers, the EU could finally respond to the criticism it has been receiving for not doing enough to protect the liberal values all over Europe, all that without actually making the already tense relationship with Russia even worse. It would also provide the EU a more separated identity from the US, being able to pursue its interests without having its main NATO ally supporting their every move. At the same time, it would be beneficial for Russia too, as this minimal form of partnership would finally provide Russia the recognition it longed for, while also granting Moscow a right to participate in the decision-making process regarding the future of Europe. Moreover, a potential partnership could prove to be extremely beneficial for both actors, as it would present great economic advantages for both sides. This partnership would also provide more incentives for cooperation on several problems, leading to the minimisation of tensions especially on topics related to their own foreign policies.

Russia should have a more important role in the Euro-Atlantic security architecture. Since the suspension of the NATO-Russia Council (NRC) in 2014, the communication between NATO and Russia has been close to inexistent, with no practical cooperation taking place since 2014 (NATO, 2020). Therefore, it would be way too idealistic to consider a scenario in which Russia, together with Ukraine, accedes to NATO, but to relieve some of the tensions and provide Ukraine better chances of NATO membership, the NRC should resume its activity. Furthermore, cooperation between Western institutions and Russia should be an objective for both sides in order for Ukraine to not represent a sensitive spot in their communication anymore.

Furthermore, in order to start a minimum form of cooperation between the EU and Russia, the two sides should incorporate more 'high-level' topics within its already existing working groups which tackle 'lower-level' politics such as environment and health. Through these strategic engagements of high-level topics into regular communication, constant contact between Moscow and Brussels could be reimplemented. As the EU is founded on a principle

of economic interdependence between its members, it should use the same principle to better its relations with Russia. Instead of focusing on their differences regarding the Eastern Neighbourhood states, they should find other areas in which they could cooperate in order to find new ways to approach their disagreements.

Conclusion

At the moment, I argue that Ukraine has overcome its problem of indecisiveness between the EU and Russia. The majority of the Ukrainian population has repeatedly expressed its support for the EU, with only some small regions of Ukraine still being pro-Russia. Nevertheless, these regions are indeed very vocal in their support for Russia, support that Russia uses to justify its significant interventions on the territory of Ukraine. Today, this is the main problem with which Ukraine has to deal with in order to have any chance at a future integration within NATO and closer cooperation with the EU. As it is still dependent on its trade with Russia, Ukraine needs to find a way to gradually detach from Russia without greatly increasing the tensions between the Russian Federation and the EU. Recent history has shown us that Russia will go to great lengths to protect its image as a world's great power, especially when it comes to direct clashes with the West. Therefore, Ukraine needs to understand that the only scenario in which it will achieve both EU and NATO memberships is with the approval of Russia. The EU will not risk military confrontation with Russia for Ukraine, and Russia will not agree to such a breach in its sphere of influence without a literal fight.

BIBLIOGRAPHY:

ÅSLUND, Anders. 2014. "The Maidan and Beyond: Oligarchs, Corruption, and European Integration." *Journal of Democracy* 25 (3): 64-73.

BROWNING, Christopher S., and Pertti Joenniemi. 2008. "Geostrategies of the European Neighbourhood Policy." *European Journal of International Relations* 14 (3): 519–51. URL: https://doi.org/10.1177/1354066108092311

DELCOUR, Laure. 2018. "Dealing with the elephant in the room: the EU, its 'Eastern neighbourhood' and Russia." *Contemporary Politics* 24(1): 14–29. URL: https://doi.org/10.1080/13569775.2017.1408169

IKENBERRY, G. John. 2018. "The end of liberal international order?". *International Affairs* 94(1): 7–23. URL: https://doi.org/10.1093/ia/iix241

KANET, E. Roger. 2018. "Russia and global governance: the challenge to the existing liberal order." *International Politics* 55(2): 177–188. URL: https://doi.org/10.1057/s41311-017-0075-3

KOETH, Wolfgang. 2014. "The 'Deep and Comprehensive Free Trade Agreements': an Appropriate Response by the EU to the Challenges in Its Neighbourhood?". *The European Institute of Public Administration*: 23–30.

MEARSHEIMER, J. John. 2014. "Why the Ukraine Crisis is the West's Fault: The Liberal Delusions That Provoked Putin. Council on Foreign Relation." *Foreign Affairs*, September/October, 2014/

MELNYKOVSKA, Inna, and SCHWEICKERT, Rainer. 2008. "Who you gonna call?: oligarchic clans as a bottom-up force of neighborhood Europeanization in Ukraine. *Arbeitspapiere des Osteuropa-Instituts der Freien Universität Berlin,*

Arbeitsschwerpunkt Politik 67. Berlin: Freie Universität Berlin, Osteuropa-Institut Abt. Politik. URL: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-439783.

NITOIU, Cristian. 2019. "Increasingly Geopolitical: EU's Eastern Neighbourhood in the Age of Multiple Crises." *Resilience and the EU's Eastern Neighbourhood Countries*: 25–47. URL: https://doi.org/10.1007/978-3-030-25606-7_2

OEC. "Ukraine (UKR) Exports, Imports, and Trade Partners." OEC. Accessed October 8, 2021. URL: https://oec.world/en/profile/country/ukr.

OLECH, Aleksander. 2019. "Determinants for the international security: membership of Ukraine in NATO."

PACER, A. Valerie. 2016. *Russian Foreign Policy under Dmitry Medvedev, 2008-2012.* Routledge.

SAUER, Tom. 2017. "The Origins of the Ukraine Crisis and the Need for Collective Security between Russia and the West." *Global Policy* 8(1): 82–91. URL: https://doi.org/10.1111/1758-5899.12374

SJURSEN, Helene and Guri ROSÉN. 2017. "Arguing Sanctions. On the EU's Response to the Crisis in Ukraine." *JCMS: Journal of Common Market Studies* 55(1): 20–36. URL: https://doi.org/10.1111/jcms.12443

SOCOLIUC, Oana-Ramona, and Liviu-George MAHA. 2019. "The Economic Dynamics of the Eastern Partnership Countries: Between Development Gaps and Internal Fragilities." *Resilience and the EU's Eastern Neighbourhood Countries*: 89–135. URL: https://doi.org/10.1007/978-3-030-25606-7_4

TERZYAN, Aram. 2020. "Closer to Europe? Domestic Changes and the Europeanization Processes in Post-Revolution Ukraine and Armenia." *Romanian Journal of European Affairs* 20 (1): 37-59.

VILSON, Maili. 2017. "Baltic Perspectives on the Ukrainian Crisis: Europeanization in the Shadow of Insecurity." *The Ideology and Politics Journal* 1 (7): 8-46.

WILSON, Andrew. 2016. "Survival of the Richest: How Oligarchs Block Reform in Ukraine." *European Council on Foreign Relations*.

WITS. "European Union Trade Balance, Exports and Imports by Country." European Union trade balance, exports, imports by country 2019 | WITS Data. Accessed October 8, 2021. URL: https://wits.worldbank.org/CountryProfile/en/Country/EUN/Year/LTST/TradeFlow/EXPIMP/Partner/by-country

DOI: 10.53477/2668-6511-22-26

THE GREAT POWER COMPETITION BETWEEN THE RUSSIAN FEDERATION AND THE UNITED STATES OF AMERICA IN THE SYRIAN WAR 2015-2020

Mara Sofia CRĂCIUNESCU,
M.A. Student in International Relations and Regional Studies, University of Tartu, Estonia.
E-mail: mara.sofia.craciunescu@gmail.com

Abstract: *Even though the Cold War ended 30 years ago, the Russian Federation and the United States of America continue the competition for power through different means and by using several instruments. The Syrian war is one of the longest and complex events in which the two states have recently exposed their capabilities. On the one hand, the Russian Federation found the Syrian war as an opportunity to improve its economy, extend its military influence and gain more allies by supporting Syrian regime and situating as a counterweight to USA. On the other hand, the United States of America fought to maintain its economic gains, strategic coalitions and limit Iran power in the region, using as motif the establishment of democracy and counterterrorism. All of these represented the most important assets of each state towards increasing their authority outside their borders and consolidating their power status in the last 6 years.*

Keywords: *The Syrian war; The Russian Federation; The United States of America; power status; terrorism; geopolitical context.*

Introduction

The Russian Federation and the United States of America are among the few states which have stood out the most on the international arena in the last century. For this reason, the great power competition between them had a fluctuating evolution and has been continuously debated. Since the end of the Cold War, the importance of nuclear capabilities has diminished and the two states had to find new ways of proving their strengths. One of the most important and recent events in which the two states have both competed and cooperated is the Syrian war.

A strong historical background of the Syrian politics influenced the uprising from 2011, known as the Syrian Civil War. Since Syria was liberated from the French rule in 1946, the state experienced multiple military coups related to the establishment of a new government. Furthermore, it started to involve in military conflicts from the Middle East, in order to develop a strong influence in the region. The current president of Syria, Mr. Bashar al-Assad, was elected in 2000. In that period, his rule was seen as a hope for democratic reforms. However, soon enough, he established an authoritarian regime and continued to support the Syrian military interventions in the neighbouring countries (Dam 2017, 56). Towards the end of 2010, the political situation in the Middle East was difficult and unstable. Within the phenomenon of "Arab Spring" multiple states, such as Saudi Arabia, Egypt, Yemen and Bahrain, encountered a lot of anti-government uprisings. All of these violent conflicts from the last century, which happened both inside and outside the territorial borders of Syria, together with the phenomenon of "Arab Spring" represented the key points for the beginning of the Syrian Civil War in March 2011.

1. The relevance of the Syrian war in the competition for power

The foreign policy of the Russian Federation and the United States of America towards the Syrian war was steady until 2014, as they were not officially involved in the conflict. Each of them supported remotely different sides, according to their interests and beliefs. However, the war developed multiple dimensions throughout time, which directly involved these two states.

Even though the Syrian uprising started with peaceful protests demanding democratic reforms, national unity and release of political prisoners, the police and army intervened at the request of the Syrian president and used live ammunition, open fire, arrested or tortured the citizens (Hinnebusch 2019, 34-37). For this reason, the civilians organised themselves in multiple groups with homemade riffles. However, they needed foreign support in order to resist (Erlich 2014, 10). Therefore, the Free Syrian Army was formed in July 2011 and became one of the most popular military opposition organisations. Its members came from multiple backgrounds: some were defectors of the Syrian Army, others were Syrian civilians and others were foreigners.

The organisation relied very much on foreign support, as the Free Syrian Army's leadership was located in southern Turkey and depended on military supplies coming from other countries (Dam 2017, 65-66). The majority of locals who tried to protest peacefully were mainly backed by the United States of America, several European states and Israel. Nonetheless, the foreign support also worsened the situation, because extremist agitators supported by Saudi Arabia and Qatar were showing a brutal response to the Syrian authorities. As the government officials from Daraa declared, the extremists shot over 1200 authorities, while Local Coordinating Committees organised peaceful protests each Friday at certain mosques. These were the only places left open by the government where people could gather. A young activist from Daraa claimed that the local tribal groups were allowed to own weapons and use them for self-defence when the authorities arrested or rushed into people's houses. However, they were not related to the sponsored rebels of Israel, United States Central Intelligence Agency or Saudi Arabia, who attacked the army (Erlich 2014, 48-50). Thus, in just few months, the Syrian Civil War had multiple sides involved in both camps, including foreign powers. However, the states involved were mainly situated in the Middle East, as the United States of America and the Russian Federation were not officially present in the conflict, yet. The fight had until that point two dimensions: a fight for freedom between the Syrian civilians and the authorities and one between the Gulf States and Turkey against Iran's expansion of power in the Middle East.

In 2012, President Barack Obama warned the Syrian President that if the army would use chemical weapons against the Syrian citizens, the United States of America will be forced to intervene militarily against the Syrian state. However, one year later, President Bashar al-Assad killed hundreds of people in Damascus with sarin gas. As a reaction, President Obama requested the Congress of the United States to approve a retaliatory missile strike, but it was refused. Thus, he negotiated with President Putin to push the Syrian President to give up these weapons. Even though the Russian Federation was an ally of Syria, it decided to ban the use of chemical weapons, in order to avoid the military intervention of the United States of America in the conflict (Wanlund 2021, 376).

Another dimension of the conflict that must be taken into account is the religious one. President Bashar al-Assad was supported by Iran, which funded and trained more than 100,000 Shia Muslims who fought alongside the Russian air force and government authorities against the Sunni Muslims and the citizens, backed by the United States of America, the Gulf States, Jordan, Turkey and Saudi Arabia (Broder 2021, 39-41). In 2013, the conflict intensified,

because there was created the powerful group named the Islamic State in Iraq and the Levant, later renamed as the Islamic State, which fought everyone, including the Kurds. The Kurds were a minority that did not belong to any country, but since 2011 they declared autonomy in Rojava, in Northern Syria. They were controlled by the Syrian Democratic Forces, but they did not join the fight against the government. Their purpose was to fight the Islamic State, which aimed to establish a united Muslim caliphate in Syria and Iraq. Thus, the religious conflict split in two subdimensions: the fight between Sunni and Shia Muslims and between the Kurds and the Islamic State (Dam 2017, 62-70). All of these events led to the official military intervention in the Syrian war of the United States of America, in 2014, and the Russian Federation, in 2015.

1.1. United States' military intervention in the Syrian war

The approach of United States of America to the Syrian war has been changing between 2015-2020, because the state had two presidents with different foreign policy approaches. President Barack Obama adopted a foreign policy based on diplomacy, rather than violence. His administration tried to have better relations with the Middle East: "a new beginning between the United States and Muslims around the world, one based on mutual interest and mutual respect", declared the president (Wanlund 2021, 375). Thus, between 2009 and 2016, the United States of America has adopted as much as possible a noninterventionist stance. Usually, in the Middle East there were few violent interventions approved by the president, which succeeded in diminishing al Qaeda's influence by keeping the American military in Afghanistan. Regarding the Arab Spring, President Obama sought to give a diplomatic response to the uprisings from Egypt, Libya, Tunisia and even Syria, by supporting the pro-democracy demonstrations and having conversations with the leaders. Eventually, the authoritarian leadership was deposed in several countries, but the situation in Syria was not the same. As I mentioned above, President Obama initially tried to resolve the conflict through diplomatic manners. However, because of the attitude of President al-Assad and the emergence of the Islamic State, the United States of America intervened military in order to establish democracy and protect human rights. In 2015, President Obama accomplished the most important action in foreign policy related to Middle East: the international agreement which limited Iran to develop nuclear weapons in return for lifting the United States' economic sanctions (Wanlund 2021, 376-377). This also had an important role in the Syrian conflict, because the limitation of the Iranian power in the region diminished the scale of the conflict.

Since 2016, the United States of America had a new administration led by President Donald Trump. His approach to foreign policy changed the relations with both Russia and Syria. He withdrew from several multilateral agreements concluded by his predecessor, including the one with Iran. Furthermore, he criticised the actions of President Obama and called them "a bad joke", while Secretary of State Mike Pompeo said that the former president showed "wilful blindness to the danger of the [Iran] regime" in his decision regarding the 2015 Nuclear Agreement (Wanlund 2021, 377). The supporters of President Trump praised his approach to foreign policy and called it successful. His realist approach of action has also improved the American-Russian relations, as he and President Putin cooperated in the Syrian war since 2016. President Trump was called "God's gift that keeps on giving", because he took advantage of the American power at international level to defend Russia or even implement its agenda (Wanlund 2021, 352-377). However, he was also criticised for his style of "one-man diplomacy" and putting the "national interest over international leadership." In 2019, after he withdrew the American military troops from Syria and let the Kurds exposed, N.A.T.O. allies questioned the integrity of the United States of America. Furthermore, Turkey and Egypt cooperated with Russia, in order to increase their armament (Broder 2021, 69-70). Apart from this, after the American troops' withdrawal, Russia concluded a ceasefire in March 2020 with Turkey over Idlib. This was the last province from Syria that was hold by the rebels (Bowen

2020). Since then, the conflict has been publicised to a smaller extent, but the regime of President Bashar al-Assad did not fall, the war is not considered as ended and there is still a catastrophic humanitarian crisis in the region, because more than half of the Syrian population has been displaced. At the end of 2020, the Syrian government still controlled the largest part of the state, but Kurdish, Rebel and Jihadist forces were also dominating significant parts of the territory (BBC News 2021). Consequently, there is an international effort to end the conflict, mostly coordinated by the United Nations, and the fall of the current Syrian regime.

The United States' intervention from the last decade in the Syrian war and overall in the Middle East was built around the United States' perception of itself. According to Blago Tashev, specialist of the Strategic Multilayer Assessment program (S.M.A.), "the U.S. sees itself as a status-quo power, maintaining a particular rules-based international order that was created by the U.S. and its allies after the World War II and is based on values shared by America and those allies" (Pagano 2017, 1). However, this order was established during the World War I, when President Woodrow Wilson advanced "The Fourteen Points" in which he emphasized the principles of self-determination and collective security. Furthermore, through his legacy, the United States of America transformed its isolationist policies into interventionist ones and involved the country in world affairs (Herring 2008, 406-407).

German Chancellor Angela Merkel described the United States' approach to international affairs during President Trump as unilateral. She claimed that by withdrawing the troops from Syria and abandoning the nuclear weapons treaty with Russia, Kremlin's position became stronger. Additionally, critics warned about the impact of president's advocacy for autocrat populist leaders, such as President Putin or the Crown Prince Mohamed bin Salman. They concluded that United States' strengths, such as diplomacy and coalitions, have been spoiled during this administration and drag down the country's status of superpower by comparing it to Russia or China. They considered that American alliances and leadership positions in multilateral organisations are important assets that keep the country above other powers. However, because they are deteriorating, the rising power of authoritarian states is facilitated and the "essential pillars of U.S. global power that have sustained Washington's hegemony for the past 70 years" are demolished (Wanlund 2021, 345-354).

Thus, several objectives of the American presence in the Middle East are focused on stability, security, economy and promoting democracy. With the help of its allies, Israel, Turkey, Jordan, Iraq, and Egypt, the United States of America fulfils the former two objectives by restraining Iranian power, countering terrorism and weapons of mass destruction. As a result of this collaboration, the economic objective is also accomplished. However, it can be observed that promoting democracy in the region is not part of the stabilisation process, as the relations with the allies are dynamic and have different interests. Thus, above all its assets, American foreign policy has a flexible approach (Pagano 2017, 2).

1.2. Russian Federation's military intervention in the Syrian war

Looking at the Russian Federation's intervention in the Syrian war, one of the main reasons that stood behind this action was its strong support for the regime of President Bashar al-Assad with whom President Putin has a good relation (Allison 2013, 796). The Russian Federation supports the territorial integrity of Syria, as well as the establishment of a peaceful life for all the ethnic and religious groups from the region (The Ministry of Foreign Affairs of the Russian Federation 2016, Section IV, para. 93). Furthermore, the Russian Federation has a specific interest in preserving the relation with Syria due to strategical reasons, as it has a naval base in Tartus and the Khmeimim air base in Latakia (See figure no. 1, Kozak 2015) (Rabinovich 2016, 3).

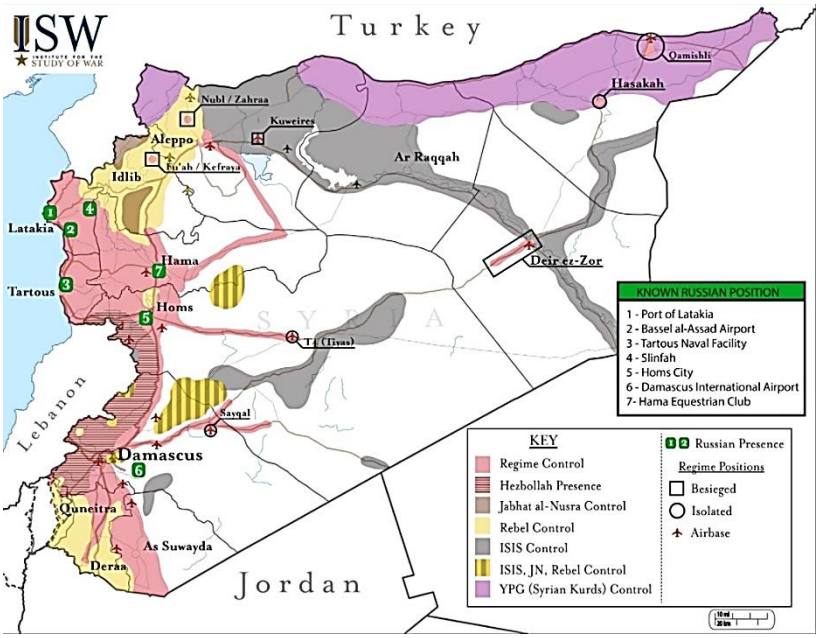

Figure no. 1: Russian Military Presence in Syria in 2015 (Kozak 2015)

In addition to this, the relationship between the Russian and the Syrian President is very important for the popularity of President Putin. If he would undermine the relation with his ally, the Russian citizens or other international supporters would question his commitment to them (Pagano 2017, 14). This consequence is something that the Russian leader would not allow to happen because it would decrease his power and, also, attack some of his personal traits, such as loyalty and hypermasculinity. Besides this, his domestic political legitimation is mostly based upon his success in external events (Taylor 2018, 40).

A second reason for its intervention was the presence of the United States of America in the region and the opportunity to grow Russian prestige in front of its opponent, because throughout history, Russia expressed its counter position over Western-led military interventions. Furthermore, Russia sees the Middle East as an opportunity to balance the United States' influence and win the race for the status of great power (Allison 2013, 796). According to the Russian Foreign Ministry, the West is imposing too much power around the world and does not allow the creation of a balanced centre of power. Furthermore, it considers that the United States of America adopted a containment policy against Russia which halts the need of cooperation in combating international challenges and destabilise international relations (The Ministry of Foreign Affairs of the Russian Federation 2016, Sections III-IV).

Another interest of Russia in the Middle East is the opportunity to grow its economy and involve in the regional market due to arms sales, nuclear technology and oil and gas benefits. The export earnings from arms sales significantly rose the budget of the country. Furthermore, President Putin has expanded its personal network in the Russian defence industry, as he appointed comrades from the Federal Security Service of the Russian Federation. Thus, his team was controlling the contracts on arms sales, which were evidently for their benefit. He had also collaborated with the main oil and gas companies in the Persian Gulf in order to establish convenient energy prices for his economic plan (Pagano 2017, 3-15).

Regarding its most recent actions in the foreign policy towards Middle East, the Russian Federation continued to pursue the national interest, by staying committed to Syria. In his last official visit to Syria, form January 2020, President Putin discussed with his Syrian counterpart about the evolution of the Syrian war and declared that there could have been observed signs of approaching an end (Presidential Executive Office 2020a). Next month, the State Duma adopted a federal law aimed at improving the military courier and postal communications

between Russia and Syria. According to the agreement, the military correspondence sent to the Russian military formations stationed in the Syrian Arab Republic is protected from border and customs control (Presidential Executive Office 2020b). In March 2020, after Russia made an agreement with Turkey on the Idlib ceasefire, President Bashar al-Assad expressed its gratitude towards the support of Russia in ensuring the territorial integrity of Syria and in fighting terrorism (Presidential Executive Office 2020c). Furthermore, in their videoconference published by Kremlin in November 2020, the two presidents declared that they succeeded in reducing terrorism in Syria and their current main priority is the return of the refugees. They both admitted that there is a humanitarian catastrophe for which there are made significant efforts, but the Syrian president declared that there is a Western embargo which does not let the government to take effective measures for helping the Syrian refugees (Presidential Executive Office 2020d). Consequently, all these recent actions present the same characteristics of Russian foreign policy mentioned above, namely consolidating peace, maintaining excellent relations with its allies, showing reluctance towards the Western world and pursuing its interest in expanding the military and economic resources, in order to raise the power status.

2. The competition for power between the United States of America and the Russian Federation in the Syrian war

The United States of America and the Russian Federation showed a serious involvement in the Syrian war, because the context and the area of the conflict reflected the interests of both states and opened a path towards strengthening their powers. Both states are in a competition to show their own capabilities and, at the same time, the weaknesses of each other. Furthermore, each of them has a different view of the whole international order because of their different approaches of international theory: liberalism versus realism.

While United States of America follows the liberalist tradition, the behaviour of great powers in the current international system is similar to the realist approach. The features which shape the system are the absence of a central authority to protect everyone, the military threat and the constant fear and mistrust among states. For this reason, powerful states try to show that they can be reliable and should become the central authority of the international system. Consequently, when it comes to wars and violent conflicts, power will be defined according to the realist perspective, namely by understanding the interdependence of multiple factors, such as culture, interest, economy, military and politics (Mondal 2014).

Therefore, the differences between the United States of America and the Russian Federation have the core in the structure of their systems. While the former is a promoter of democracy, which invests in defence and has a solid economy, the latter has an opposed regime, which relies on energy exports and foreign policy legitimacy, as its economy is unidimensional and eight times weaker than the American one (Pagano 2017, 8). Nevertheless, the Russia Federation is the sixth in the world at the level of purchasing power. Thus, even though it does not reach the same levels of the United States of America, the Russian Federation's economy should not be underestimated. However, from the military point of view, there is a tough competition between the two. Regarding the military budget in terms of purchasing power, the Russian Federation officially spends approximately 65 billion dollars, but, according to Dimitri Simes, advisor of former United States Presidents R. Nixon and D. Trump and CEO of the Centre for the National Interest, the numbers of the Russian military budget may, unofficially, reach between 140-150 billion dollars (Simes 2021). Even though the United States of America has officially declared a military budget of 732 billion dollars, the manpower in the Russian Federation is much cheaper than in the United States of America. Likewise, while the United States of America have more naval ships and aircrafts, the Russian Federation possesses more

battle tanks and, in terms of GDP, it has a higher defence spending percentage than Americans (Russell 2021, 4). Thus, each of them has different assets.

The Middle East, this diverse area with multiple conflicts which pressured the United States of America in various ways, seemed ideal for ambitious Russia to pursue its interests of involving in serious foreign affairs, cooperate with other influential powers against the United States of America, while becoming, apparently, the mediator of conflicts from Middle East. According to their official policies, the two states share the same interests in countering terrorism and nuclear security. However, they support opposing factions in the Syrian war. For example, The Russian Federation had an efficient cooperation with both allies and rivals of the United States of America, in order to attract them to the Russian side. On the one hand, the Russian Federation allied with Syria and Iran and helped them in terms of weaponry, in order to fight better the United States of America and Israel. On the other hand, it took the advantage of the broken relations during the Arab Spring between the United States of America and Egypt and Saudi Arabia and helped them through diplomatic and military manners. The Russian Federation also had an influence on Israel, in order to drive it away from its dependence on the United States of America and has also built good relations with Palestine throughout history. Thus, by analysing the religious dimension of the Syrian war at the moment of its intervention in the conflict, the Russian Federation was an ally of both Shia and Sunni Muslims until 2015 and its role in the Middle East suffered only small changes (Rabinovich 2016, 3-4). This plan, to ally with as many regional powers as it could, emphasized the interest of Russia to weaken American relationships with Middle Eastern countries and its influence in the region. Thereby, the Russian Federation could gain more support in the domestic and regional public opinion in terms of its strength and diplomatic leadership, while the perceptions about the United States of America would be more negative (Pagano 2017, 3).

Nevertheless, the administration of President Putin showed a similar approach of the Syrian conflict to the one of President Trump, as the American President said himself at the beginning of his term that the relation between them will thrive. "Getting along with Russia is a good thing, not a bad thing", declared President Trump (Wanlund 2021, 356). Since the end of the Cold War and until his presidency, all the American Presidents tried to ease the tensions between the two countries. However, they did not succeed due to the Russian influence over the former Soviet states, where the American influence was also trying to expand. Taking into consideration that they helped each other in multiple situations, the good relation between the two leaders was not a surprise. However, N.A.T.O.'s actions towards the Russian Federation did not show similar "friendly" intentions. The organization sent more troops near Russian Federation's borders in Poland and the Baltic States and, also, gave deadly weapons to Ukraine, actions which President Obama would have not made, claimed Professor Henry Nau, former member of the National Security Council. Furthermore, the United States of America imposed sanctions on the Russian Federation for its invasion in Ukraine and even for its support for President Bashar al-Assad and other actions related to terrorism (Wanlund 2021, 356-358).

The Russian Federation claims that its policy is non-ideological, like the American one which tries to promote democracy and, at the same time, weaken the stability of the region by strengthening extremist factions that threaten Russian security. Thus, from a Russian point of view, its role is to stabilise the balance of power from the region by trying to voice its opinions and advance its policies at the same level as the United States of America. From a Western point of view, the non-ideological involvement of the Russian Federation in the Middle East represents, however, a confrontation with the United States of America. As the Russian Federation is using soft power to gain influence in the region, it might overstep United States' goals. For example, building close relations with many states from the region (including United States' allies) and also with non-state actors (considered by the West as terrorist affiliated) or influencing aspects from regional politics, tourism and education might actually affect the

stability of its relationship with the United States of America. For this reason, the United States of America has a proactive approach and comprehensive policies instead of immediately reacting to the Russian Federation's actions. On the same note, the United States of America is, first of all, focused to accomplish its national interests of containing Iranian power and countering terrorism from the region. Thus, its strategy does not include the Russian Federation as a threat, but rather accepts its presence in the region (Pagano 2017, 18-19).

Russia's foreign policy towards the Syrian war showed its reluctance towards any Western-led military interventions in the region. The Concept of the Foreign Policy of the Russian Federation from 2013 outlined Russia's strong support for the Syrian regime and stood up for rejecting any foreign military intervention within the state, arguing that it might destabilise international peace. Emphasizing its position as a permanent member of the United Nations Security Council and its aim of settling global and regional problems, Russia considered the measures taken by the West towards Syria as illegitimate and threatening. Therefore, it claimed that the Western intervention consisted in coercive measures which infringed upon the United Nations Charter and were not helpful in resolving the crisis. "Such measures only lead to the expansion of the conflict area, provoke tensions and arms race, aggravates interstate controversies and incite ethnic and religious strife", stated the official document (The Ministry of Foreign Affairs of the Russian Federation 2013, Section II, para. 15). The same motivation to settle conflicts could also be observed in the last Concept of the Foreign Policy of the Russian Federation, published by the Ministry of Foreign Affairs in 2016. In this document it was emphasized the aim of Russia to cooperate with the international community in combating international terrorism, as well as to consolidate global peace and security and settle a fair and democratic international system in accordance with the provisions of the Charter of the United Nations and under the organisation's management of international relations. Another significant purpose mentioned in the document is strengthening the position of the state "as a centre of influence in today's world". In Russia's view, this purpose together with its "open and predictable foreign policy" and its historical stateliness in counterbalancing the evolution of international affairs, determine the independent and assertive foreign policy based on following the national interests of the state (The Ministry of Foreign Affairs of the Russian Federation 2016, Sections I-III).

However, there is a possible cooperation between the two countries if the tensions among Middle Eastern powers would amplify so much that only a fusion between Russian and American powers would stabilise it. At the moment, the United States of America insists on the regime change in Syria as this might be the only solution. However, it does not provide more details about which alternative for the government might be better. For this reason, both the United States of America and the Russian Federation should focus more on countering terrorism and providing help regarding the security of the citizens. By analysing the situation on short-term consequences, if they succeed in diminishing the disputes, they would support a stable governance in the region. Neither of them is interested in prolonging the regional disputes, so this might be an optimistic scenario in which they might reach an agreement (Pagano 2017, 4-7). Furthermore, the Russian Federation declared that is open to collaborate with the United States of America for international security as long as their relationship is "based on mutual trust, respect of each other's interests and non-interference in each other's domestic affairs" (The Ministry of Foreign Affairs of the Russian Federation 2016, Section I, para. 72). However, as I mentioned that the Russian Federation is not hurrying to counter the terrorism from the region until Syria is fully protected, the cooperation with the West might remain unlikely to happen.

Conclusions

The great power competition between the Russian Federation and the United States of America clearly evolved during their intervention in the Syrian war. While the former strongly followed its national interests to have a successful foreign policy that would improve the political legitimacy of the president, the latter was involved more ideologically. Consequently, the American-Russian relationship from the Syrian war portrays the opposing interests and actions of each other in the region, while the two countries did not interact directly with each other.

Besides the different traditions they follow, realism for Russia and liberalism for the United States, both are supporting different sides in the Syrian war. As I have already mentioned above, the Russian Federation backed the groups from Syria and Libya, which fought against the United States of America. Thus, the Russian presence in the region aimed tightening the relations with regional powers and investing in military operations, which would weaken the American influence. Expanding its military capabilities in the region was a very important goal for the Russian Federation because it brought more benefits than a remote cooperation would have done on the long term. On the contrary, the United States of America weakened the relationships with some of its allies, such as Turkey. However, it accomplished other goals, such as defending its economic interests from the region and the expansion of Islamic radicalism.

From the ideological point of view, their relation had a fluctuating evolution. During the administration of President Obama, the Russian Federation was sceptical about the American presence in the region but cooperated with it for limiting chemical weapons in Syria because it was its own interest. However, the situation changed during the administration of President Trump. The similarities between President Trump and his Russian counterpart's approach to foreign policy helped them to limit the international attention toward the conflict. Their cooperation was also very important for the development of the states outside the Syrian war.

While the United States of America aimed mainly to spread democratic values and back the civilians, the Russian Federation supported the regional governments and their authoritarian characteristics. As the civilians did not have the power to influence the order of the conflicts and most of the states complied better with Russia's style of action rather than the Western approach, Russia's bandwagoning strategy was welcomed by several regional powers. Even some of United States' allies gained interest in Russia's presence and moved to its side. However, it is important to mention that the attitude of the Middle Eastern states towards the United States of America was influenced by the fluctuating number of resources received during the two American presidential administrations in-between 2012-2020. For this reason, the future of the Russian Federation's advantages in the Middle East still depends upon the Western interest in the region. Nevertheless, the Russian Federation holds nowadays an important position, at least regionally, and is involved in a war that started ten years ago, which might have another uprising when and if democratic forces from around the world will decide to intervene and re-establish the order in the region. However, the multipolar world of today does not let the United States' rule to overcome other states' powers. The neoliberal system encourages everyone to cooperate for common benefits and until it will change, there will always be multiple strong states, which will dominate together the international affairs.

BIBLIOGRAPHY:

ALLISON, Roy. 2013. "Russia and Syria: explaining alignment with a regime in crisis." International Affairs 89, no. 4 (Oxford University Press): 795-823. URL: https://doi.org/10.1111/1468-2346.12046

BBC News. 2021. "Why has the Syrian war lasted 10 years?" March 12, 2021. URL: https://www.bbc.com/news/world-middle-east-35806229

BOWEN, Jeremy. 2020. "Syria war: Russia and Turkey agree Idlib ceasefire." BBC, March 5, 2020. URL: https://www.bbc.com/news/world-middle-east-51747592

BRODER, Jonathan. 2021. "U.S.-Iran Relations: Is a Military Conflict Inevitable?." In Global Issues, 120-174. SAGE.

DAM, Nikolaos VAN. 2017. "Destroying a Nation. The Civil War in Syria." I.B. Tauris.

ERLICH, Reese. 2014. "Inside Syria: The Backstory of Their Civil War and What the World Can Expect." Prometheus Books.

HERRING, George C. 2008. "«A New Age»": Wilson, the Great War, and the Quest for a New World Order, 1913-1921". In From Colony to Superpower. U.S. Foreign Relations since 1776, 378-435. Oxford University Press.

HINNEBUSCH, Raymond. 2019. "What Went Wrong: Understanding the Trajectory of Syria's Conflict". In Syria: From National Independence to Proxy War, edited by Linda Matar & Ali Kadri, 29-52. Palgrave Macmillan. URL: https://doi.org/10.1007/978-3-319-98458-2

KOZAK, Chris. 2015. "Russian Posture in Syria: September 27, 2015." Institute for the Study of War. http://www.understandingwar.org/map/russian-posture-syria-september-27-2015

MONDAL, Puja. 2014. "Power of Politics: Meaning, Types and Sources of Power." Your Article Library. Accessed April 20, 2021. URL: https://www.yourarticle library.com/essay/power-of-politics-meaning-types-and-sources-of-power/31356

PAGANO, Sabrina J. 2017. "Alleviating US-Russia Tensions." Arlington, VA: Strategic Multi-layer Assessment (SMA) Reach-back Cell. URL: http://nsiteam.com/sma-reachback-R4.7_Alleviating_US_Russia_Tensions/

Presidential Executive Office. 2020a. "Vladimir Putin posetil Sirijskuju Arabskuju Respubliku." January 7, 2020. http://kremlin.ru/catalog/countries/SY/events/62545

Presidential Executive Office. 2020b. "Podpisan zakon o ratifikacii soglašenija meždu pravitel′stvami Rossii i Sirii o sotrudničestve v oblasti voennoj fel′d″egersko-počtovoj svjazi." March 2, 2020. http://kremlin.ru/catalog/countries/SY/events/62895

Presidential Executive Office. 2020c. "Telefonnyj razgovor s Prezidentom Sirii Bašarom Asadom." March 6, 2020. http://kremlin.ru/catalog/countries/SY/events/62956

Presidential Executive Office. 2020d. "Vstreča s Prezidentom Sirii Bašarom Asadom." November 9, 2020. http://kremlin.ru/catalog/countries/SY/events/64358

RABINOVICH, Itamar. 2016. "The Russian-U.S. Relationship in the Middle East: A Five-Year Projection." Carnegie Endowment for International Peace, April 5, 2016. URL: https://carnegieendowment.org/2016/04/05/russian-u.s.-relationship-in-middle-east-five-year-projection-pub-63243

RUSSELL, Martin. 2021. "Russia's armed forces Defence capabilities and policy." European Parliamentary Research Service. URL: https://www.europarl.europa.eu/thinktank/en/document.html?reference= EPRS_BRI%282021%29689370

SIMES, Dimitri. "What is the «Great Game» between Russia and the United States? The Bottom Line." Interview by Steve Clemons. *The Bottom Line*, Al Jazeera English, May 6, 2021. Video, 16:11. URL: https://www.youtube.com/watch?v=45KvUGnfmrg

TAYLOR, Brian D. 2018. "The Code of Putinism." Oxford University Press.

The Ministry of Foreign Affairs of the Russian Federation. 2013. "Concept of the Foreign Policy of the Russian Federation." Approved by President of the Russian Federation V. Putin on February 12, 2013. URL: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/122186

The Ministry of Foreign Affairs of the Russian Federation. 2016. "Foreign Policy Concept of the Russian Federation." Approved by President of the Russian Federation V. Putin on November 30, 2016. URL: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

WANLUND, Bill. 2021. "U.S. Foreign Policy in Transition: Is the United States relinquishing its global supremacy?" In Global Issues, 344-406. SAGE.

DOI: 10.53477/2668-6511-22-27

SPECIAL OPERATIONS FORCES IN UNITED NATIONS PEACE KEEPING OPERATIONS

Octavian DACIN,
Colonel **(**Ret.), MA in Security and Defense, Military Academy of Armed Forces "Alexandru cel Bun", Chisinau, Republic of Moldova.
E-mail: dacinoctavian@gmail.com

Abstract*: Special Operation Forces had started to participate in the United Nations peacekeeping operations not long ago, but the consensus on acceptability of their use in peacekeeping operations has already been reached. Present article analyzes views on SOF use in peacekeeping, as expressed by the specialist and enshrined in guidance documents of different countries, explores normative regulation formalized in mandates of respective peacekeeping operations and contemplates typical SOF tasks in peacekeeping operations as defined by the UN in "United Nations Peacekeeping Missions Military Special Forces Manual".*

Keywords*: peacekeeping operations; United Nations Organization; Armed Forces; special operation forces; area of operation; SOF operators.*

Introduction

Offering the widest range of capabilities that have direct applicability in a large number of environments, the Special Operations Forces (SOF) are most often the preferred option of political-military decision-makers. SOF actions differ from the actions of conventional forces due to political risks, mode of action, mode of involvement, independence from their own forces and increased dependence on the information and means of indigenous forces (General Accounting Office /NSIAD-97-85).

The SOF includes in its composition specialized structures, from all services and branches of armed forces, which are organized, equipped and trained to carry out specific missions. The methods of training are specific to perform a wide range of missions, which sometimes include deliberate acceptance of risk or covert missions that are part of the range of operations executed by conventional forces.

The participation of special operations subdivisions in peacekeeping operations is a relatively recent practice. For the first time, the SOF were used in peacekeeping operations under the scenario proposed by the UN Secretary-General Dag Hammarskjold, which implied refraining from intervening in the internal affairs of the host countries, not using forces other than those for self-defense, and maximum transparency of the peacekeepers' actions. As the current North Atlantic Treaty doctrine states, the characteristics of the SOF require a wide range of significant applications in peacekeeping operations, but their open use in an unstable political environment can lead to emotional reactions (Allied Joint Publication 3.4.1., 2001). Traditional peacekeeping operations did not imply the involuntary appearance of missions commonly associated with those of the SOF (reconnaissance, destruction/capture of objectives behind enemy lines, organization of partisan movements, training of host units and so on), during the conduct of the service by peacekeepers, so the issue of the admissibility of SOF's participation in peacekeeping operations was not current at the moment.

1. SOF operators' competences in peacekeeping operations

With the end of the Cold War, SOF's participation in peacekeeping operations and other types of multinational operations intensified. As David S. Maxwell wrote in 1995, U.S. special operations forces in one form or another participated in the main UN operations of that time, such as: in northern Iraq, Somalia, Rwanda, Cambodia and Haiti, but in each individual case they were applied differently. In Iraq, they were initially used to assess the area of operations and prepare the entry of following forces, then as a result – as a subordinate task force, to coordinate interaction with the civilian population in the area of responsibility, in a similar way as conventional peacekeepers. In Somalia, they ensured the safety of air transportation with humanitarian aid, then carried out the safety of communication and interaction with the UN forces through the "coalition support groups", organized interaction with the civilian population in the area and finally took part in hostilities. In Haiti, they trained UN forces units, delegated from its composition "coalition support groups", organized information programs and interaction with the civilian population in remote areas (Maxwell 1995). SOF played an important role in NATO operations in Bosnia. They delegated coordination and liaison teams to the staff of all non-NATO units to support and maintain compatibility with the multinational division's staff in ensuring communications, reconnaissance, fire support and evacuation of the wounded. SOF operators provided aid in EOD operations, acted as observers of joint committees, and carried out reconnaissance missions in the interest of the command in the area of responsibility (Bohle 1997, 17). In all these operations, SOF operators did not wear blue helmets, were not included in the composition of the UN peacekeeping contingents, did not hold the status of UN peace maintainers and did not act according to the legal-international framework governing UN peacekeeping operations.

In the literature of the 90's, emphasis is made on the possibility of SOF's participation in UN operations, not on their ability to carry out special reconnaissance and conduct combat operations, but by applying their skills in traditional peacekeeping missions. Thus, Franklin C. Bohle and David S. Maxwell define a series of competences of SOF operators: maturity and experience (Bohle 1997, 4), knowledge of foreign languages, cultural sensitivity, capacities in obtaining information, ensuring the access of Allied forces to communications, intelligence and fire support through "coalition support groups" (Bohle 1997, 35). From the above we can conclude, that SOF operators can carry out missions to obtain information, ensure interaction between multinational forces, train local forces to ensure security and carry out high-precision strikes in favor of the peacekeeping forces command (Bohle 1997, 15).

SOF`s operator deep knowledge of regional culture and foreign languages, as well as the presence of experience of interaction with local forces, are stipulated in the U.S. Armed Forces leadership documents on peacekeeping operations – JP 3-07.3 (Joint Publication 3-07.3. 2018). In the previous version of this document, were established missions for special operations forces in the peacekeeping operations of the United States, such as: carrying out psychological operations; collection of information; ensuring the detailed assessment of specific areas; interaction with the Armed Forces and the local civilian population, with other peacekeeping contingents and agencies; training and organization of security forces; use of aircraft and helicopters (Joint Publication 3-07.3. 2018, II-9). According to NATO's peacekeeping doctrine, the ability of SOF operators to cover large areas in secret, with secure communication, allows them to act quickly, immediately after the establishment of liaison, recognition and other missions. SOF operators can also organize civil-military interaction with the local population, ethnic communities in the area, to inform them and also train and reform local security forces (Allied Joint Publication 3.4.1. 2001, 5-7).

The basic document governing the activities of the British Armed Forces in the field of peacekeeping operations is AJP-3.4.1(A) *The Military Contribution to Peace Support*

Operations. The three basic missions of the SOF: observing and reconnaissance; offensive operations (to achieve the calculated and precisely concentrated effect, physical or psychological, with minimum damage); support and influence (including the preparation of 'third parties' and/or the provision of influence over them; the "mastery of the minds and hearts" of the native population, influencing it, through information operations), can be carried out both in peacetime and in wartime, or during a conflict, together or separately. This category also includes any other missions that contribute to implementing the operational plan of the peacekeeping forces command, such as: the completion of civil-military projects and the fulfillment of the duties of military observers in conditions of high-tension situation (Maxwell, 1995, 5-21).

Western experts are not alone in their view of the opportunity of SOF operators' participation in peacekeeping operations. In 2000, specialists from the Russian Federation already included reconnaissance missions for special operations in peacekeeping operations and medical humanitarian aid operations, without detailing the missions during such participation (Freze 2000, 4).

2. SOF operators' application in peacekeeping operations

Taking into account the above, we can divide two approaches to the application of SOF in peacekeeping operations:

– "Moderate", suggesting the use in peacekeeping operations of the skills characteristic to SOF operators without changing the essence of peacekeeping operations (US, NATO).

– "Radical", involving a change in the essence of peacekeeping operations under the aegis of the UN: the acceptance of covert actions and the extensive use of force, which will make it possible to apply the combat skills of SOF operators on a large scale (UK).

– What approach is typical for peacekeeping operations under the United Nations aegis? Existing trends allow us to state that peacekeeping operations under the UN aegis are typically the second option, the "radical" one, because several changes are observed in the conduct of peacekeeping operations, namely:

– the expansion of missions (from the maintaining the traditional peace to maintaining a multidimensional peace);

– expanding cases of the use of force and an increase in the level of force applied (from self-defense to defending the mandate, from maintaining traditional peacekeeping to robust peace enforcement).

The works cited above, written by Franklin C. Bohle and David S. Maxwell in 1995-1997, did not describe the combat experience of the UN`s "blue helmets". Meanwhile, the changes in the 2000s necessitated radical changes in the use of peacekeeping forces, which were completely unimaginable at the time of the " Agenda for Peace "drafting. These changes also found room for special operations forces in the UN peacekeeping contingents.

The first case of the application of SOF operators as part of the UN peacekeeping force (and not interacting with "blue helmets") took place in Burundi. In his resolution of 16 March 2004, the UN Secretary-General defined that it is necessary to include SOF operators in the peacekeeping contingent for the successful completion of the mission (First report of the Secretary-General on the United Nations Operation in Burundi S/2004/682). For setting up the UN peacekeeping operation in Burundi (hereinafter – ONUB), troops from the African Union mission in Burundi (hereinafter – AMIB) were deployed, which included South African SOF operators. South Africa agreed to send them to the ONUB until their replacement arrived (Overview of Secretary-General's Reports, S/2004/210). SOF operators also participated in the UN peacekeeping mission in Darfur, 31 July 2007 (hereinafter – UNAMID). SOF operators in

Nepal characterized themselves as "a vital element, allowing reserve forces to respond quickly to the mission threats." (Resolution 1769 2007).

The next additional step in the development of the practice of applying SOF operators in UN peacekeeping operations became a mission in Congo (hereinafter – MONUC, then reformed in MONUSCO). The commander of the MONUC mission P. Cammaert thus characterized the features of this mission. For the first time in the history of MONUC peacekeeping UN aegis formed... plus an enormous number of helicopters, impressive engineering capabilities and special operations forces for conducting military action in accordance with Chapter VII (UN Charter 1945) problematic region of the Republic of Congo. This represents a global change in peacekeeping, as a result of which the UN receives adequate military means for the execution of a mandate of coercion with strict rules for the use of force, which implies a more aggressive position of UN troops and a higher tempo of use, which sometimes leads to a deadly character (CAMMAERT 2010). The Special Operations Forces were an integral element of the UN strategy in Congo that used them without hesitation.

The actions of MONUC SOF operators differed drastically from the usual way of UN peacekeepers action. On January 18, 2006, MONUC dispatched its SOF operators from Guatemala to Garamba National Park, receiving information about the alleged presence of militants from the "Liberation Army of the Lord", including commander V. Otti, whose arrest warrant was issued by the International Criminal Court. On 23rd of January, as they approached the militants' camp, MONUC SOF operators came under their fire, as a result of which eight peacekeepers were killed and five were injured (Joint Publication 3-07.3. 1999, 8). That situation provoked drastic debates about how much the international community is willing to go with military methods, in order to maintain peace in the DR Congo ().

The failure described above did not result in the termination of the use of SOF operators by the UN in Congo. On the contrary, this failure led to the adoption of the UN Security Council resolutions 2098 (2013) of 28 March 2013, for their use. According to this resolution, the UN Security Council established a "Task Force" as part of the UN Stabilization Mission in Congo (MONUSCO), the component of which included a reconnaissance company and a special operations company. This brigade was intended to neutralize militant groups and had a mandate to: "conduct offensive operations in a harsh, highly mobile and diverse environment, in strict accordance with the standards of international law, including international humanitarian law and the UN human rights audit policy in support of non-UN formations, prevent the expansion of all armed groups, neutralize the expansion of all military groups, to reduce the threat they pose to state power, to ensure stabilization of activities and civilian security in western areas of the DRC"[1].

Resolution 2098 (2013) played a critical role, both in the practice of UN peacekeeping operations and in the practice of using SOF operators in them. This resolution provides for UN peacekeepers, in general, and SOF operators, in particular, the greatest freedom at the moment for the use of force. Sometimes the peacekeepers acted in this way, but their aggressiveness in actions was never dealt at the level of the mission's mandate – its fundamental document. Most of the legal-international impacts on the use of SOF operators in combat and reconnaissance operations were removed, and the remaining restrictions relate to how combat operations are conducted. From the above, we conclude that Resolution 2098 (2013) provided these changes in duties only for the operators in the SOF company, as part of the "Operative Intervention Brigade". For the other SOF operators in the composition of the MONUSCO forces, the attributions remained unchanged, according to the contingent mission (Security Council SC/10964, 2013).

[1] A.N.: Search engine for the United Nations Security Council Resolutions, S/RES/2098, URL: http://unscr.com/en/resolutions/2098

Another mission of the UN peacekeeping contingent with the participation of Dutch SOF operators was the United Nations integrated mission on stabilizing the situation in Mali (hereinafter – MINUSMA). Mandate 2100 (2013) MINUSMA of 20 April 2013 put before the peacekeepers the mission "in support of the transition authorities in Mali to provide stabilization of the situation in the main localities in the region, especially in northern Mali and as a result to repel threats and take active measures to prevent the return of militant elements to these areas, which allows UN peacekeepers the option to take preventive-active actions (Security Council resolution 2100, 2013).

As the situation in Mali got complicated day by day, proposals were put forward to reform the MINUSMA mission. According to the vision of the MINUSMA mission commander, the contingent of UN peacekeepers, who should act in establishing and maintaining peace, was confronted with the activities of terrorist networks in the region and fought against them, without having the proper mandate, the necessary training, equipment, logistical provision and intelligence.[2] Mali's foreign minister proposed to the Security Council "within a time-frame as soon as possible to review the mandate of MINUSMA and strengthen their capacity and resources so that they can cope with the outbreak of violence in the country... " Perhaps the Council should review the question of the establishment of 'Operational Reaction Forces', which maintain a potential to fight terrorists.[3] There is no doubt that the change of MINUSMA's mandate to one for the fight against terrorism would imply more operational freedom for its contingent of SOF operators.

The situation in the area of responsibility of the UN integrated mission to the Central African Republic (hereinafter – MINUSCA) looked not so sad, but the mission required the involvement of SOF operators (Security Council 2014). The mandate of S/RES/2149 (2014), MINUSCA, of 10 April 2014 provided the mission "to ensure, within the limits of its capabilities and the areas of deployment, including active patrolling, the protection of the civilian population against physical violence."[4] As a result, we can see that even the harshest wording of the mandate would not bring a positive result, if the mission staff would not be active in the execution of such mandate.

In the absence of detailed regulation of the SOF operators use in UN peacekeeping operations, their missions are described in detail in the "Handbook on Special Operations Forces for UN Peacekeeping Missions" issued by the Department of Peacekeeping Operations and the Field Support Department. It provides a definition for the concept of *UN Special Operations*: "military actions carried out by special formations, organized, trained and equipped decently, supplemented with selected personnel, using unconventional tactics, techniques and methods of action. These actions may be carried out within the framework of a wide range of UN peacekeeping operations, in accordance with the principles and spirit of peacemaker, and in the context of the mission's mandate ".[5] UN special operations can be carried out at different stages of the mission: at the initial stage, while SOF operators can achieve favorable conditions for the full deployment of the mission, stabilization and protection of the civilian population, and finally, during peace-building, when they can ensure advanced training and the development of opportunities for the armed forces of the host country.

[2] A.N.: This was a meeting on the report of the Secretary-General on the situation in Mali, S/PV.7274, URL: https://www.securitycouncilreport.org/un-documents/document/spv7274.php

[3] A.N.: This was a briefing on peacekeeping operations by force commanders from MONUSCO, MINUSMA and UNDOF, S/PV.7275, URL: https://www.securitycouncilreport.org/un-documents/document/spv7275.php

[4] Letter dated 29 January 2015 from the Secretary-General addressed to the President of the Security Council, S/2015/85, https://undocs.org/S/2015/85

[5] United Nations Peacekeeping Missions Military Special Forces Manual // DPKO – DFS, January 2015, http://www.enopu.edu.uy/wp-content/uploads/manual-UNMUM-Special-Forces-2015.pdf, p.9.

One of the criteria for establishing the missions for UN SOF operators is the compliance of these missions with the mandate and legal framework of the UN operation, including the rules of engagement. Particularly, the rules regarding using force must be formulated taking into account the specific missions of UN SOF operators.[6]

3. UN SOF operators' basic missions

Special Surveillance and Reconnaissance (SR) – they complement the effort and the system of collecting information at national level and the theaters of operations, by obtaining significant, specific, very well defined and time-bound data and information at the strategic and operational level. Surveillance and reconnaissance missions can complement other collection methods, when there are certain constraints dictated by weather conditions, difficult terrain, hostile countermeasures, etc. Special surveillance and reconnaissance is a predominant function of Human Intelligence (HUMINT), which has the ability to place "eyes on the target" in a hostile, forbidden or politically sensitive territory. The Special Operations Forces can provide timely analysis by using the initiative and their own method of evaluation in a way that other technical procedures are not possible. They can carry out these missions independently, supported or in conjunction with/for the benefit of other categories of forces/component commands and can use reconnaissance and surveillance techniques, advanced equipment and methods to collect data and information, sometimes supplemented by indigenous means.

SR specific activities include the following:

– *Environmental Reconnaissance* These are operations carried out for the collection and reporting of critical geospatial data and information, including hydrographic, geological, geographical and meteorological.

– *Threat assessment.* Threat assessment should be based on accurate and timely information whenever possible.

– *Specific Assessment.* These are operations carried out to detect, identify, locate and assess a target, in order to determine the greatest efficiency in the use of different weapon systems. This type of operation may also include assessing the potential effects (including collateral damage) of the target's engagement.[7]

Direct Actions (DA) are high-precision operations, limited in purpose and duration. Direct actions normally involve a planned withdrawal from the area in the immediate vicinity of the objective; focus on specific, well-defined targets of strategic or operational value or in the context of decisive tactical operations. Special Operations Forces can conduct these types of missions independently or with the support of conventional forces.

Direct actions include the following:

– *Raids, ambushes, direct assaults*. These operations are intended to achieve specific, well-defined and often time-sensitive results. They are sometimes beyond the actual capabilities of hitting elements of conventional forces. Such operations typically involve attacking critical targets, disorganizing the Lines of Communications (LOC), capturing personnel, models of military equipment and armaments, conquering, destroying/neutralizing enemy capabilities or facilities.

– *Routing operations for the target engagement*. These are operations carried out to identify and report the precise location of target to enable non-organic SOF platforms to use high-precision weapon systems. This includes any type of electronic, mechanical or voice

[6] *Ibidem*, p.14.
[7] United Nations Peacekeeping Missions Military Special Forces Manual // DPKO – DFS, January 2015, http://www.enopu.edu.uy/wp-content/uploads/manual-UNMUM-Special-Forces-2015.pdf, p.17.

communication, which provides the aircraft/weapon system to be used with additional information about the specific location of a target.

– *Personnel recovery operations.* These are operations performed to search, locate, rescue and bring back to your own personnel, sensitive equipment, or critical elements for the security of a state in combat areas or areas controlled by the enemy. SOF recovery missions are characterized by detailed planning, numerous rehearsals and a thorough informative analysis. These types of operations use unconventional tactics and techniques, a discreet crawl and the frequent use of ground teams.

– *Precision damage* are operations in which collateral damage must be minimized. In this type of operations, highly sophisticated precision weapons or the scheduled initiation of specific quantities and types of explosive substances are used, located in exact locations to achieve the mission's objectives. Precision destruction operations can be carried out against targets on which weapon systems using high-precision guided ammunition do not guarantee success from the first hit, or when what contains a particular facility must be destroyed without causing damage to the entire facility.[8]

Military assistance (MA) is a broad set of measures in support of friendly forces throughout the conflict spectrum. Military assistance may be carried out by, with or through friendly forces that are trained, equipped, supported or used to a varying extent by the SOF. The extent of military assistance is considerable and can range from the provision of military training to material support for the engagement of indigenous forces active in major operations, if the mission's mandate also allows for consideration of UN human rights audit policy. Military assistance activities may include the following:

– *Training*. This represents a complex of activities of training the soldiers and units of the host nation Armed Forces in the use at the tactical level, of supporting and integrating the combat skills; provides specific advice, assistance and training to military leaders in the use of tactics, techniques and techniques to strengthen the host nation's potential to protect itself against threats and to develop the necessary individual and organizational skills.

– *Counseling*. These are activities that strengthen the security of the population by offering an active participation in tactical level operations carried out by the host nation military units with the aim of neutralizing insurgent threats, isolating the insurgents from the civilian population and protecting it (United Nations 2015).

Conclusions

From the above we can conclude that:

– SOF operators have gone a route from unimaginable to the need to include them as an essential component of the United Nations peacekeeping contingents. The UN Security Council supports the practice of using SOF operators in peacekeeping operations by approving the relevant reports of the Secretary-General and, in the case of Resolution 2098 (2013), directly supporting the inclusion of SOF operators in the "Operational Intervention Brigade" component of the MONUSCO mission. Expanding the range of action of peacekeepers and the legal cases of the use of their force, provides more and more opportunities to use the specific skills of SOF operators. The current trend gives reason to an increase in the participation of SOF operators in peacekeeping operations.

– The mandates of the MISSIONS ONUB, UNAMID, MINUSCA, MINUSMA and MONUSCO differ from each other, but SOF operators are an important component of each of these missions. Most UN special operations can be carried out within the framework of each

[8] *Ibidem*, p.18.

mandate of current UN missions along with an armed contingent of peacekeepers. The specific wording of the mandate (e.g. MONUSCO's mandate) may "untie loose hands" in the actions of SOF operators, but it is not a mandatory condition for their use in the appropriate missions.

– The use of UN SOF operators requires some standardization of use, legal explanations, or a concept of their alternative status to be presented, which would provide, on the one hand, the UN with an instrument of power and, on the other hand, non-involvement of the "ordinary" peacekeeping staff in the conflict.

BIBLIOGRAPHY:

North Atlantic Treaty Organization. 2001. Allied Joint Publication 3.4.1. Peace Support Operations.

BOHLE, Franklin C. 1997. Army Special Forces: a Good Fit for Peace Operations / Franklin C. Bohle // United States Army War College. – Carlisle Barracks, Pennsylvania, ASIN: B0006QP4MC.

CAMMAERT, Patrick, major-general, Former UN Military Adviser and former Division Commander, MONUC, URL: https://www.ipinst.org/images/pdfs/favoritapaper/favoritacammaert.pdf

United Nations. 1945. Charter of the United Nations, URL: http://www.oas.org/XXXIVGA/English/reference_docs/Carta_NU.pdf

United Nations Security Council. 2004. First report of the Secretary-General on the United Nations Operation in Burundi S/2004/682. URL: https://undocs.org/ru/S/2004/682

General Accounting Office. NSIAD-97-85 Special Operations Forces – Opportunities to Preclude Overuse and Misuse.

Reliefweb. 2006. Guatemalan Blue Helmet Deaths Stir Congo Debate. URL: https://reliefweb.int/report/democratic-republic-congo/guatemalan-blue-helmet-deaths-stir-congo-debate

United States Joint Chiefs of Staff. 1999. Joint Publication 3-07.3. Peace Operations.

United States Joint Chiefs of Staff. 2018. Joint Publication 3-07.3. Peace Operations.

Joint Doctrine & Concepts Centre. 2004. Joint Warfare Publication 3-50. The Military Contribution to Peace Support Operations.

United Nations Security Council. 2015. Letter dated 29 January from the Secretary-General addressed to the President of the Security Council, S/2015/85, https://undocs.org/S/2015/85.

MAXWELL, David S. 1995. Support to United Nations Operations: Is There a Role for United States Special Operations Forces, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, First Term AY 95-96.

Security Council. 2004. Overview of Secretary-General's Reports, S/2004/210, URL: https://www.securitycouncilreport.org/un-documents/document/burundi-s2004210.php

Security Council. Overview of Security Council Meeting Records, S/PV.5784, URL: https://www.securitycouncilreport.org/un-documents/document/sudan-spv5784.php

Security Council. 2006. Overview of Secretary-General's Reports, S/2006/390. URL: https://www.securitycouncilreport.org/un-documents/document/drc-s2006390.php

Security Council. 2007. Resolution 1769 (2007) / adopted by the Security Council at its 5727th meeting, on 31 July 2007, S/RES/1769 Darfur (UNAMID). URL: https://digitallibrary.un.org/record/604309

Security Council. 2013. Resolution 2100 [on establishment of the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA)]. URL: https://www.refworld.org/docid/519dffbe4.html

Security Council. 2014. Resolution 2149 [on establishment of the UN Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA) until 30 Apr. 2015]. URL: https://www.refworld.org/docid/537c6ea64.html

Security Council. 2013. Security Council SC/10964, Authorized as Security Council Grants Mandate Renewal for United Nations Mission in Democratic Republic of Congo – Resolution 2098. URL: https://reliefweb.int/sites/reliefweb.pdf

Security Council. 2014. Meeting on the report of the Secretary-General on the situation in Mali, S/PV.7274. URL: https://www.securitycouncilreport.org/un-documents/document/spv7274.php

Security Council. 2014. This was a briefing on peacekeeping operations by force commanders from MONUSCO, MINUSMA and UNDOF, S/PV.7275. URL: https://www.securitycouncilreport.org/un-documents/document/spv7275.php

United Nations. 2015. United Nations Peacekeeping Missions Military Special Forces Manual //DPKO – DFS, January 2015. URL: http://www.enopu.edu.uy/wp-content/uploads/manual-UNMUM-Special-Forces-2015.pdf

FREZE V.R., KUZIN V.N., KOTKOV S.A. 2000. Sputnik razvedchika: [uchebno-metod. posobie], pod red. M.L. Tihomirova-Novosibirsk: Novosibirskij voennyj institut. URL: https://www.twirpx.com/file/1448724

DOI: 10.53477/2668-6511-22-28

SEPARATISM TODAY: THE GEOPOLITICALLY SIGNIFICANT CASE OF CATALONIA

Anamaria MANOLE,
BA student in Security Studies, Faculty of Political Science, University of Bucharest, Romania.
E-mail: aem.manole@gmail.com

Abstract*: Catalonia's national identity has its roots in the Middle Ages and Early Modern Times. In the 19th century, the Catalonian search for independence was encouraged by romantic and revolutionary concepts spread across Europe. After the First World War, we can notice a significant increase of political actions as regards the Catalonian nationalists-separatists, including violent episodes and riots in main cities. As for the contemporary period, the financial crisis in 2007-2008 acted as a new booster for nationalist-separatist ideas leading eventually to referendums in 2009 and also in 2017. The present study is exploring in a historical register the process of Catalonian's independence. In doing so, I intend to identify and examine the Catalan's main reasons in claiming complete political independence. The study tackles particularly recent interviews presenting opinions of several Catalonian citizens, some of them with political or administrative responsibilities, concerning regional independence and its potential consequences.*

Keywords*: Catalan's national identity; political independence/autonomy; politico-territorial controversy; contemporary conflicts.*

Introduction

The kingdom of Spain is a European state in south-western region of the continent, well known for its exports of fruits, vegetables, olive oil, wine, medication, etc. across the globe. Since the fourth decade of the 20th century tourism, industry and agriculture became the main pillars of the country's economy.

It is one of the oldest European countries, which encompassed all of its present-day territory by 1512. The state-building occurred under monarchical government prior to the rise of nationalism, and this could help explain the continuing salience of territorial identities and the periodic willingness of the political centre to permit territorial elites to retain some prior privileges and separate laws (Henders, 2010, 50).

The construction of national identity in terms of ethnicity has been ruled out as in most European countries. Even so, there is not really just one national image with which the Spaniards identify themselves; there are many different ideologically and territorially based conceptions of the country (Solis, 2003, 11).

Nowadays, Spain is a parliamentary democracy and constitutional monarchy, even it has experienced- and still experiences, as we'll see along this study- conflicts over the territorial distribution of political authority, due to asymmetries of history, language, identity, socioeconomic factors and geography.

In this paper, my intention is to do research through the historical course of the 20th and 21st century regarding the rising of nationalism in the region of Catalonia. Assuming that I will succeed in doing so, I will also try to find the main reasons which led the Catalans to claim for

complete political independence. My research is focused on three directions of analysis, as it follows: 1. Historical background of Catalanism in the 20th century; 2. The nationalist movements of Catalans in the 21st century; 3. Opinions of several Catalonian citizens regarding the independence of their region.

1. Historical background of Catalanism in the 20th century

Back in the 18th and the 19th centuries, territorial identity claims along with conflicts over the secularization and class interests were politically salient in Spain. In the late 19th century, the central state of Spain had been weakened by ideological conflicts, besides the loss of the Spanish Empire and economic stagnation (Henders, 2010, 51). This might be how the first explicitly Catalan nationalist program took place: they wanted to distance themselves from the Spanish problems and by this ground they decided to create a new ontology rooted in their culture, language and worldview.

In 1914 it was established the Catalan Regional Government (*Mancomunitat de Catalunya*) based on the so-called *Bases de Manresa.*, considered as the "birth certificate of political Catalanism", at least that of conservative roots. Among its forecasts, the third base says that t*he Catalan language will be the only one that can be used officially in Catalonia and in the relations of this region with the central power* (Foguet, Boreu, 1966, 272). In the fourth base, we remark that *Only Catalans, both those by birth and those who are by naturalization, may hold public office in Catalonia, including government and administrative positions that depend on the central power (*Foguet, Boreu, 1966, 272). Also, in the sixth base it is said that *Catalonia will be the only sovereign of its internal government, therefore it will freely dictate its organic laws; It will take care of its civil, criminal, commercial, administrative and procedural legislation; establishment and collection of taxes (...)* (Foguet, Boreu, 1966, 273). By this point, Catalans managed to accomplish few of their aspirations for decades.

Until the mid-1920's Catalanism was a middle-class conservative movement which carried out a policy of cooperation with the Central Government – as example, the actions of *Lliga Regionalista,* founded in 1901, which pleaded for an ambitious project involving both Catalonia and Spanish State-. Since 1923, Primo de Rivera – who served as a prime minister of Spain – was struggling to abolish the catalan official institutions, like the *Mancomunitat de Catalunya* – deliberative assembly that advocated the federalization of Spain. The dictatorship managed to disband and outlaw it in 1925. Although this assembly had only administrative functions, it represented the first recognition of Catalan identity and territorial unity by Spaniards since 1714, being also responsible for the creation of many public institutions in health, culture, technical education and science and notably for the support of the Catalan language.

In 1936, Spanish Civil war broke out as an outcome of polarization of Spanish life and politics that had developed over previous decades: on one side, the Nationalists – were most Roman Catholics, important elements of the military, most landowners, and many businessmen –, and on the other side, Republicans – were urban workers, most agricultural labourers, and many of the educated middle class – (Editors of Encyclopaedia Britannica, 2021). Also in that period the Catalan statute was implemented, establishing the *Generalitat* made up of a Catalan parliament, president and executive council (Henders, 2010, 51). In the same year, Francisco Franco Bahamonde was appointed as *Generalissimo* (a military rank of the highest degree) and Head of State, also holding the function of leader of Bando *nacional* (Nationalist faction). By consolidating all nationalist parties into a one-party state (*FET y de las JONS),* he succeeded in declaring Nationalists victory in 1939, thus and so his dictatorship was extended over Spain through a period of repression of political opponents. After the war, the Franco regime

abrogated the autonomy statutes, making the suppression of public expressions of territorial identity a pillar of its political program. Until 1943, the regime banned Catalan language from public use, destroyed their books and patriotic monuments. He prohibited university classes and institutions dedicated to Catalan culture, banned the Catalan flag, anthem, and national dance (Henders, 2010, 51). Many individuals who resisted were fired, fined, jailed or forced into exile. (Conversi, 1997, Ch5, 155-158). *Culturally, Franco's regime imposed on the country an official version of Spain and Spainishness based on uniformity and homogeneity, seeking the root out all traces of cultural and ideological differences* (Solis, 2003, 21). In later years, the regime allowed public expressions of Catalan identity in only specified controlled situations (Henders, 2010, 51). Throughout these harshest years of the dictatorship in Spain, the fight for Catalan identity recognition was a difficult one, as it was the struggle for democracy. Furthermore, this period of repression convinced Catalan political elites that *democratization required the recognition of territorial-cultural difference and that territorial self-rule would not be restored without democratization* (Henders, 2010, 55).

After Franco's death in 1975, the tension about the identity problem gathered new momentum with the development of the State through the setting in progress of a democratic Constitution. So on, after the ending of the dictatorship, with the whole country united behind one democratic objective, a plurality of viewpoints re-emerged. The distribution of territorial and political authority gave birth to antagonistic visions over the new democratic state. One of them was referring to the unitary nature, centralization and homogeneity along the lines of the modern state and citizen model, while the other one cantered around the open way for a federalized, decentralized and even asymmetrically organised Spain. In this regard, Art. 1 of the Constitution established a single sovereignty, *residing in the Spanish people, from which the powers of the State emanate*, emphasizing the *indissoluble unity of the Spanish nation, common and indivisible patria of all Spaniards* (Agencia Estatal Boletín Oficial del Estado, 1978). By contrast, Art. 2 recognized and guaranteed *the right to autonomy of the nationalities and regions of which it is comprised* (Agencia Estatal Boletín Oficial del Estado, 1978). Thus, by speaking of nationalities and regions, the contradictions encountered in the first articles of the Constitution implied differences amongst Spain's territorial communities and individual citizens.

Spanish political elites wanted to secure a democratic transition partly by agreeing to give special status to Catalonia who had an active nationalist movement claiming the territory and a distinct identity due to its language, which was maybe one the most important aspects that have been preserved even in the toughest times along the history. By the time of Franco's death, about 78 percent of Catalonia residents still claimed to speak Catalan. As I said before, the post-Franco Spanish Constitution allowed groups of historical provinces across the country to form Autonomous Communities with organic laws (Statutes of Autonomy). The Catalan AC was established with the most expensive competencies possible by means of the first two articles of the Constitution mentioned before, enjoying a high level of self-rule through its institutions (a parliament, government and Premier) known collectively as the *Generalitat* (Real Instituto Elcano, 2015, 18). The Community has been ethnolinguistically diverse, considering the fact that in 1981 about 35 percent of its 5.1 million residents were born outside Catalonia, which meant that those individuals had identities different from Catalan natives. Therefore, their interests didn´t interspersed with the native Catalans; for example, their economic concerns were about their low-status derived from lower-paid occupations, while Catalans were concerned about economic development across their region after the Franco era (Henders, 2010, 58-86).

Only two weeks after more than one million Catalans participated in the *Diada* (Catalan's National Day) in 1977, they succeeded in restoring the *Generalitat*, and two years later the *Cortes* (Spanish parliament) approved their autonomy statute. Subsequently, in the

eighth decade of the 20th century, few of the long-term targets of the historical region of Catalonia were accomplished: The Spanish Constitution recognized Catalan as a regional language co-official with Castilian (Generalitat de Catalunya, 2019), the central government had less control over the regional government, Catalonia had its own largely autonomous police forces and more autonomy in matters of tax and fiscal autonomy. So the Catalan special status arrangement contributed to the successful transition to a democratic state. Afterwards, controversy surrounding the autonomy statute had tested the stability of the arrangement, for its provisions appear to push Spain towards greater levels of political decentralization because of the recognition of multiple nations, and this fact was about to challenge the modern territorial state and citizenship model (Moreno Fernandez, 1986, 157-170).

2. The nationalist-separatist movements of Catalans in the 21st century

In order to find an explanation for the nationalist-separatists movements in the contemporary period, we should take a look at how the political sphere influenced the emergence of manifestations. According to Michael Keating (1994, 39-59), there are three explanations of the emergence of nationalism in the region of Catalonia: first of them is based on an ethnic dimension, which has a stronger presence through last centuries; the second one is based on the will of the people; the third one explains the emergence of nationalism as an instrument of a political elite seeking to create a state through a nationalistic appeal. Even if there is a long story behind the construction of Catalan's inclusive nationalism, its foundation does not seem like being created by just one of the three explanations, but strongly developed by political elites together with the citizen's cravings and their feeling of belonging to a distinct nation.

I will focus, as I consider it is one of the most important research areas for this paper, on the Catalan territorial politics. This politics have been dominated by political parties representing various intensities and varieties of nationalism and a range of ideological orientations. From 1980 until 2003, the region was governed by Center-Right Christian Democratic *(Unió del Centre i la Democràcia Cristiana de Catalunya, UCiDCC)* and moderate nationalist coalitions led by Convergence and Union (*Convergència i Unió*, CiU*)* – a party well-known for his influence in reference to the independence of Catalonia, by its leader Jordi Pujol, who used to defend the notion of Catalonia as a nation within Spain – (Carrera, 2014, 77). In 2003, the CiU lost control to the Socialist Party of Catalonia *(Partit dels Socialistes de Catalunya, PSC–PSOE)*, which formed a coalition with the independence-supporting Catalan Republican left *(Esquerra Republicana de Catalunya, ERC)* and with Green-Initiative for Catalonia United (*Iniciativa per Catalunya Verds, ICV)*. Even so, CiU remained the party with the most seats in the Catalan parliament.

In 2004, the elections changed the course of politics, with Luis Rodriguez Zapatero as the leader of the party who took over the government – Spanish Socialist Workers Party – *(Partido Socialista Obrero Español, PSOE).* After this, Catalonia's Tripartit coalition announced the plan of elaborating a new Statute for their region, which seemed to be supported by Zapatero; the statute was asking, among other things, for Catalonia to be recognised as a political nation, for a new economic agreement system and for the establishment that the *Generalitat* will collect all of the state taxes from the first year and will have regulatory capacity over them (El pais, 2005). In 2005 a civic platform of more than 700 organizations of any kind was created in Barcelona with the name *Plataforma pel dret a decidir* (Civic Platform for the right to decide); its first major event demonstrations took place in 2006 (Vilaregut Sáez, 2011, 330), while the proposal referring to the new Statute was negotiated in Madrid. Despite

obtaining 74% of the vote in a referendum, participation was below 50%, but maybe with the support of pro-independence and federalist parties, the Statute was approved.

2010 was the year when the Constitutional Tribunal ruled against the Statute, cutting most of its crucial articles. In July of the same year, the Catalan civil-society organization *(Xarxa Òmnium)* organized a demonstration under the slogan *Som una nació, nosaltres decidim!* (We are a nation and we have the right to decide!), which received the support of labour unions, many civic society organizations and political parties, with a turnout of more than a million people (BBC News, 2010). Even though in November of the same year CiU returned to power, in November 2012 the strongly pro-independence party *Esquerra Republicana de Catalunya* won the elections.

Since 2012 the idea of holding a referendum for independence has had a central place in Catalonia, with some parties in favour of it (Turp, Caspersen, Qvortrup, 2017, 12). It was the time when *Assemblea Nacional Catalana* (Catalan National Assembly) was created as an activist civil -society organization, whose purpose was the reaching of independence through democratic and peaceful means -; it was made of nearly 500 regional groups and played a key role in organizing the informal referendums. The first time when Catalan government tried to hold a formal referendum in order to become an independent republic took place in 2014, but it was blocked by law and declared as illegal by the Spanish government. Due to the provisions of the Constitution of Spain, which gave wide autonomy to the regions but affirmed the indissoluble unity of the Spanish nation. Instead of a referendum, Catalan president of that time -Arthur Mas- proposed a process of citizen participation, as an alternative to the referendum but the Spanish government announced that it would also block it. However, the Catalan government holded the ''informal non-binding vote'', in defiance of the Constitutional Court. This manifestation together with the major march which took place on 11 September (when Catalans are celebrating their national day) marked the initiation of the sovereignty process.

In 2013 the Parliament of Catalonia adopted by a large majority the "Declaration of Sovereignty and of the Right to Decide of the Catalan People", but in 2014 this act was declared by the Spanish Constitutional Court as being unconstitutional, and the Congress of Deputies rejected the authorisation of an independence referendum. Even so, the Generalitat began its own parallel consultation, which was, as expected, prohibited by the Constitutional Court (Boletín Oficial del Estado, 2014, 1-4). The 2015 Catalan regional elections were framed as a proxy for an independence referendum by the pro-independence parties; after an election campaign dominated by the independence issue, the results delivered a majority of seats in the Parliament but yet not a majority of votes (Marti, Cetrà, 2016, 107-119).

In 2016 Carles Puidgemont was elected as the Premier of the Generalitat, even if at that time he was a relatively obscure politician whose candidature had been promoted by hard-line supporters of the independence movement (Real Instituto Catalano, 2019, 22-26). Since that moment, the strategy to break with Spain was accelerated by the well-known self-determination referendum and the unilateral declaration of independence. The referendum took place in 2017, despite prohibitions by various courts and the day was dominated by the coercive action of riot police trying to prevent voting in some institutions. Pro-referendum posters widespread by more than 700 mayors were seized by the police, considered as illegal and criminal. The Spanish Government also threatened with the financial takeover of the Catalan budget (Baquero, 2018). The following days saw a strong reaction from the upholders of the Spanish Constitution who organised anti-independence protests in Barcelona; at this point the King Felipe VI of Spain gave a televised speech in which he accused the Generalitat of acting *on the margins of the law and democracy* (Holodny, 2017). In the same year, even so the political and social tensions were running high, the pro-independence groups in the Catalan parliament issued a unilateral declaration of independence with the support of just 70 of the 135 members of parliament, and so it had no impact and no international recognition. The same day, the Spanish

Government triggered Article 155 of the Constitution, which assumed that if an Autonomous Community will not fulfil the obligations imposed upon it by the Constitution or other laws, there will be necessary the Spanish Government to step in self-rule, fully dissolving the Catalan Government and Madrid scheduling new regional elections (Agencia Estatal Boletín Oficial del Estado, 1978, 47). So it happened: the so-called "Spanish Constitutional Crisis" (known as the Catalan crisis) ended by invoking the article of Constitution that I've mentioned before. The Spanish government imposed direct rule over Catalonia, ending its autonomy and seizing control of the entire government institutions and infrastructure. Furthermore, the Spanish government began to prosecute a case against several of the autonomous region's leaders, as well as the organizers of the referendum. In the very next year, nine of the Catalan independence leaders were sentenced to prison.

In the spring of 2018 there was established a new government under the president Quim Torra - a pro-independence politician -. In 2019, the Barcelona-El Prat airport was forcibly closed because of the violent protests which took place; the reason was that the Spanish Court decided to send in prison several leaders of the independence movements which illegally unfolded two years before (Cordero, 2019). Regarding this, Torra called for an immediate halt to violence and suggested peaceful protests. Shortly thereafter, taking into account that violent protests branched out for many days, the Catalan president attempted to rally the crowd of protesters by stating that he would initiate a new independence referendum. Thus in October few minor trade unions linked to the pro-independence movement called for a general strike involving other violent clashes between masked protesters and police. After several days and nights of violence, Torra asked for talks between the Catalan independence movement and the Spanish Government, but the head of the Spanish government refused as he stated that it was impossible under Spanish law (Burgen, Jones, 2019).

The last two years came as a challenge for all countries around the world because of the emergence of Covid-19 as a global pandemic. But this fact didn't stop the Catalans from carrying out protests, at least on Catalonia's National Day. The 2020 Diada manifestation was a protest adapted to safety measures imposed by authorities due to the pandemic. Close to 60.000 people attended static protests across the region. In 2021, the Catalan National Assembly was the organizer of the event. It was estimated that over 400.000 people expressed their willingness to participate, but Barcelona's local police estimated the attendance at about 100.000. So the world crisis brought changes not only in health and economy but it also brought a "wave of calm" for the nationalist-separatists citizens of Catalonia, even if the relationship between Catalan Government and Spanish Government seem to endeavor in establishing a consensus regarding the statute of Catalonia.

3. Opinions of several Catalonian citizens regarding the independence of their region

As I said in the beginning of this paper, I initiated a survey containing 9 questions, which were physically handed over to a number of seventy citizens of Catalonia. Some of the questions had predefined answers, some of them required answers based on the considerations of the respondents. The language used to conduct the survey is Catalan, precisely to help respondents understand exactly what answers to give. The reason why I chose respondents from different fields of work is that I considered it would be a better way to find out if there are contrasts among their opinions. In this regard, taking into account the fact that in Catalonia there is currently a number of approximately 7.5 million inhabitants, the number of 70 chosen respondents represents 0.0009% of the total. Although the chosen sample does not represent a large enough part of the population to be able to form an exact opinion, they come from different backgrounds, live in distinct areas of Catalonia and have different social statuses. Of the total

number of respondents, 45.71% are female, and the remaining 54,29% are male. Also, the respondents can be divided into 4 categories, depending on their age: those aged between 18 and 25 are 25.71%; those aged between 25-35 are 45,72%; in the category 35-55 years are 22,85% of the sample; last but not least, those aged between 55 and 65 are 5.72%. Regarding education, 97.14% attended at least high school education, 75.71% of respondents attended university, while only 47.14% did their masters or doctoral school.

At least, I divided the seventy respondents in five groups, based on their status of employment, as follows: unemployed citizens – 10% of the respondents –, employees in the field of agriculture – 11.43% –, employees in the field of economy – 25.72% –, employees in the field of public authorities – 37.14% –, and employees in the legal field – 15.71%. In the following I will describe my findings after collecting and analyzing all of the answers. This last division will be used as a general statistic to represent the answers to the nine questions.

For the first question "Do you consider yourself Spaniard or Catalan?", there are 2 answer options: 1. Catalans, 2. Spaniards. 68.57% of the respondents answered that they consider themselves Catalans and 31,43% answered that they are Spaniards. According to gender, 42.86% of women and 57.14% consider themselves Catalan. Regarding the age criterion, the first answer was chosen as follows: 100% of the first age category; 87.5% of those aged between 25-35 years; 31.25% of those aged 35-55 years; 0% of those aged 55-65 years. As the results show, we can see that the young tend to support the nationalist-separatist principle more than the elderly. Is it a pure desire for separation or is it simply a faith they have acquired from those who campaign for independence? We can observe in Figure 1. the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	57,14%	87,5%	72,22%	57,69%	9,09%
Answer 2	42,86%	12,5%	27,28%	42,3%	90,91%

Figure no. 1

There are two answers for the second question "Were you and your family born in Catalonia or another region?": 1. Catalonia, 2. Other regions. The percentages show that 77.14% of the respondents came from Catalonia and the rest of 22.85% belong to other regions like Castile de Leon, Galicia, Andalusia and Murcia. In the gender category, 57.40% of women and 42.60% of men chose the first answer. Regarding the age, we can see that the rate of people aged between 18 and 35 born in Catalonia is much higher than people aged 35-65 years, as follows: for the age category 18-25 there is a percentage of 100%; people aged between 25-35 are born in Catalonia in a proportion of 96.88%; those in the age category 35-55 are in proportion of 31.25%, and the last age category has a percentage of 0%. We can observe in Figure 2. the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	42,86%	62,5%	88,33%	84,62%	81,82%
Answer 2	57,14%	37,5%	16,67%	15.38%	8,18%

Figure no. 2

The third question "Have you participated in a public protest supporting the independence movement?" had two answer options: 1. Yes, 2. No. The answer revealed that only 25.71% of the respondents participated in an independence movement, while the rest of 74.29% didn't. A percentage of 21.88% of the total number of women respondents and 28.95% of the total number of men participated in a protest for independence. Regarding age, we can see that, young people tend to show greater support for pro-independence movements: 66.67% of young people aged 18-25 participated in public events; 27.78% of those aged between 25-35 years and only 5.56% of those aged between 35-55 years; the last age group showed no interest in participating in the protests. I also think it is important to take a look at the percentages according to education: 50% of the people who chose the first answer attended at least high school; 44.44% attended university and in the category of those with postgraduate studies only 5.56% showed an interest in the independence movement. We can observe in Figure 3. the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	28,57%	75%	27,78%	11,54%	18,18%
Answer 2	71,43%	25%	72,22%	88,46%	81,82%

Figure no. 3

On the fourth question "How do you think a pro-independence protest should unfold?" the respondents had to choose one of the following 3 answers: 1. Violent protests, 2. Pacifist protests, 3. Protests shouldn't exist. None of the respondents think that violent protests should exist. 63.64% of the respondents chose the second answer, 44.29% consider that these events shouldn't exist. The second answer was chosen as a percentage of 51.28% of the total number of women and 48.72% of the total number of men. The third answer was chosen by 38.70% of women and 61.30% of men. Regarding age, we can see that younger people show support in the existence of protests, while older people say they should not exist. Thus, the existence of protests is supported by 88.88% of those aged between 18-25 years, for the category 25-35 there is support in a percentage of 65.62% and from those aged between 35-55 there is support in proportion of 12.5%; the last age category does not consider the existence of protests necessary. A percentage of 11.11% of those aged between 18-25 opted for the third answer; 34.38% of those aged between 25-35; 87.5% of those aged 35-55; 100% of those aged 55-65. The educational level shows that the support for protests is 98.47% for those who attended high school, 79.58% of those who attended university and 48.71% of those who did postgraduate studies. Those who claim that the protests should not exist attended 100% a high school, 70.96% a university and 45.16% postgraduate studies. We can observe in Figure 4. the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	0%	0%	0%	0%	0%
Answer 2	100%	100%	72,22%	30,76%	36,37%
Answer 3	0%	0%	27,78%	69,24%	63,63%

Figure no. 4

The fifth question "Do you agree with the independence movements of Catalans?" had two answer options: 1. Yes (plus a possible continuation of the answer), 2. No (plus a possible continuation of the answer). The percentage shows that 61,43% of the respondents agree with the independence movement. Few of their most common reasons to agree such a thing are: "Yes, because it is a very rich region that should not depend on a larger state.", "Yes, because I was born here and I see a bright future for such a developed region.", "Yes, because a large part of the area's revenues is taken over by the Spanish state.". Few of their common reasons to agree with the second answer option are "No, because it violates European standards.", "No, because the region could not govern itself.", "No, because such a small state does not have enough resources to support itself". In the gender category, the percentages show that 90.63% of women and 36.84% of men agree with the independence movement. Regarding age, we can see a decrease in support for pro-independence movements as they get older: in the first category of young people aged between 18-25, 94.44% have a pro-independence attitude, those aged between 25-35 in proportion of 59.37%, those aged between 35-55 in proportion of 43.75% and the last age category is in total disagreement. It is interesting that out of the total number of people who support the demonstrations for independence, 100% attended a high school, 88.37% attended a university and only 27.90% of them also attended postgraduate studies; so, as the level of education increases, support for independence decreases.We can observe in Figure 5. the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	42,85%	75%	72,22%	69,23%	36,37%
Answer 2	57,14%	25%	27,77%	30,77%	63,63%

Figure no. 5

For the sixth question "Do you agree with the fact that Spain does not approve independence?", there were two answer options: 1. Yes (plus a possible continuation of the answer), 2. No (plus a possible continuation of the answer). The results show a big percentage of agreement, 71.43%. 18.57% opted for the second answer. Few of the most common reasons to agree with the fact that Spain does not approve independence are:" Yes, because I agree with European values." or "Yes, because Spain does not have to divide.". Among their reasons to disagree, the most common are: "No, because they should also see the needs of the regions, not just those of the Spanish state." or "No, because in this way it violates the right to choose of the Catalan community.". The positive answer to this question seems to be the clear choice of older people. In this sense, it is necessary to observe the percentages for the first answer. 65.62% of the total number of women and 94.73% of the total number of men agree with the attitude of the Spanish government. The percentages in the age category show us that people aged between 18-25 years agree in a percentage of 50%, those aged between 25-35 years are in percentage of 87.5% and people aged between 35-55, respectively 55-65 agree in proportion of 100%. Regarding the level of education, 100% of those who chose the first answer have at least finished high school, 87.72% have completed university studies and 45.61% attended postgraduate studies. In Figure 6. we can observe the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	71,43%	50%	77,78%	88,46%	90,91%
Answer 2	28,57%	50%	22,22%	11,54%	9,09%

Figure no. 6

For the seventh question, "Do you think that Catalonia deserves independence?", there were two answer options: 1. Yes (plus a possible continuation of the answer), 2. No (plus a possible continuation of the answer). The results show a small percentage of agreement, 24.59%. and a big percentage of disagreement, 75.71%. Through the most common arguments for the first question we can find: "Yes, because it has its own language and traditions.", or "Yes, because the struggle for independence has been a great desire of Catalans in recent decades.". For the second answer, the most common reasons to disagree with independence are: "No, because in this way the provisions of the Constitution would be violated." or "No, because there would be the possibility for the new state to enter into an economic collapse.". Women who chose the first answer are 18.75% and men are 28.96%. The percentages according to age show us again an increased support for independence from young people, as follows: 72.22% of those who chose the first answer are people aged between 18-25 years, 12.5% are people with ages between 25-35 years, and the last two categories have a support percentage of 0%. Respondents have the following levels of education: 94.12% attended high school and college, while only 17.45% attended postgraduate studies. In Figure 7. we can observe the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	28,57%	75%	22,22%	7,69%	9,09%
Answer 2	71,43%	25%	77,78%	92,31%	90,91%

Figure no. 7

For the eighth question "Do you think that Catalonia's independence can bring it a lasting development?" respondents had two answer options: 1. Yes (plus a possible continuation of the answer), 2. No (plus a possible continuation of the answer). The results show that only 15.71% of the seventy respondents opted for the first answer. The second answer was chosen in a proportion of 84.29%. The most common reasons for choosing the first answer were: "Yes, because we have enough economic resources to ensure sustainable development." or "Yes, because our incomes based on agriculture are really big.". Through the most common arguments brought for the second option, we can find: "No, because even if the region has sufficient resources for development, it would be too difficult for our leaders to manage this." or "No, because if Catalonia gained independence, it would leave the European Union, so the economic system would have to be completely changed.". Although support for pro-independence demonstrations appears to be significant (see answers to question 5), respondents to this question seem to be aware of the realities of the environment in which they live. Thus, in the gender category, only 9.36% of women and 21.05% of men believe that eventual independence could provide an environment which can lead to long-term development. According to the age criterion, 50% of the respondents aged between 18 and 25 years, respectively 6.25% of the respondents aged between 25-35 years chose the first answer; people

aged between 35-55 and, respectively, 55-65 totally disagree with the idea that Catalonia would have a development if it separated from the Spanish kingdom. Also, the degree of education shows that 100% of the respondents who chose the first answer option attended at least one high school, 63.63% also attended university studies, and 36.36% attended postgraduate studies. In Figure 8. we can observe the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	42,85%	37,5%	16,66%	3,85%	9,09%
Answer 2	57,14%	62,5%	83,33%	96,15%	90,91%

Figure no. 8

The last question was "Do you think that independence will one day become a reality?". The respondents had two answer options:1. Yes (plus a possible continuation of the answer), 2. No (plus a possible continuation of the answer). The results show that a very small part of the respondents believes in such a thing, 11.43%. The rest of 88.57% opted for the answer "No". Among the most common arguments brought to the first answer, we can find: "Yes, because there is a strong Catalan spirit that fights for this ideal" or "Yes, because the protests will not stop until the independence goal is achieved". The most common reasons for choosing the second answer are: "No, because it violates European democratic standards." or "No, because the Spanish state would never accept this". It seems that the last question can give us a clearer picture of the respondents' opinions. Thus, in the gender category, 3.13% of the total women and 18.42% of the total men consider that independence is an achievable aspect. In the age category we can see once again a greater support from young people than from older people: 33.33% of people aged between 18-25 and 5.56% of people aged between 25-35 chose the first answer option; none of the respondents in the 35-55 or 55-65 age categories believe that independence is achievable. The level of education shows that 100% of the respondents who believe that independence can be obtained attended a high school, 87.5% attended university, but none of them attended postgraduate studies. In Figure 9. we can observe the data sorted by their social status.

Categories	Unemployed	Agriculture	Economy	Public Authorities	Legal field
Answer 1	28,57%	25%	16,67%	3,85%	0%
Answer 2	71,43%	75%	83,33%	96,15%	100%

Figure no. 9

Conclusions

Following what is presented in this paper, it appears that the Catalan nationalist-separatists exist in several social categories, not only in the favoured or in the least favoured, from a social point of view.

From what I understand so far, the idea of autonomy was first introduced by political elites who saw potential in the geographical area of north-eastern Spain. Later, spreading this ideal among the citizens, they appropriated it and began to believe in a good organization of the region as a distinct part of Spain. However, Catalan citizens over the age of 35 understood,

probably due to their experience in the environment in which they live, that Catalonia's independence would not be as constructive as it may sometimes seem. Even if there are still people in the population who have a high level of education and support independence, the percentage is too small to be taken into consideration. Linguistic and traditional differences have probably been a bonus for increasing autonomy support, but even if these differences exist, people with a sufficiently high level of education and work and social experience have become aware that they don't have enough arguments to separate a region from the rest of the state.

From the same perspective, we can look at the demand for independence, which was clearly not propagated for the first time by the citizens of Catalonia, but by its political leaders, who overestimated the capacity for development in the event of possible independence. The citizens welcomed with open arms the idea of possible independence, especially if we consider that it is a region that is distinguished from the rest of Spain by certain characteristics that have stood out throughout history. However, polls show that the ages of respondents who claim that the Catalan region should be independent are generally under 35, which leads me to believe that this nationalist-separatist spirit is rooted only in the minds of young people who have born at the end of the 20th century or at the beginning of the contemporary era and that this ideal is spread only by those in this category precisely due to a lack of political and social experience.

In my opinion, mass protests and the use of illegal demonstrations or the use of violence began to develop when Spain used its organs of authority and the rule of law to stop growing support for independence. This shows us that, even in the 21st century, some aspects of a political nature cannot be understood by all societies. First, the political elites who have supported independence since the beginning of the 21st century tend to forget the exact provisions of the Constitution. Given that the population, in general, takes over political attitudes and behaviours induced by leaders and their ideals, some Catalan citizens have assimilated this desire for independence and turned it into an ideal they have shared with some political leaders. In fact, from my own research and discussions with people of Catalan nationality I have come to the conclusion that the youth category is most likely to act inappropriately in protests, just to draw more attention to the cause they support.

Personally, I consider the Catalan ideal to be unfeasible, given that the above surveys also show little support for the independence of the region. Even if some young people consider this to be something worth fighting for by any conventional or less conventional methods, their arguments are insufficient to make them a reality. I also believe that by re-establishing internal relations between Spain and Catalonia, communication between the two could lead to a consensus. Given that the Catalan region will be able to identify real reasons for achieving full independence, the Spanish Kingdom probably could not refuse its request. But given the lack of real reasons for demanding independence, it will remain an unfulfilled ideal, probably just like a simple thought in the memory of young Catalans.

BIBLIOGRAPHY:

Agencia Estatal Boletín Oficial del Estado. 1978. "The Spanish Constitution". UEL: https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf

BAQUERO, S., Camilo. 2018. "New Catalan government sworn in, paving way for suspension of direct rule". URL: https://english.elpais.com/elpais/2018/06/02/inenglish/1527944812_829249.html

BEIZSLEY, Daniel. 2021. "Young Catalans wanted a country. They'll settle for a steady paycheck", accessed September 7, 2021. URL: https://www.politico.eu/article/spain-catalonia-independence-movement-youth-unemployment-identity-nationalism/

BURGEN, Stephen; JONES, Sam. 2019. "Catalan president calls for talks with Spain's government after unrest", accessed September 3, 2021. URL: https://www.theguardian.com/world/2019/oct/19/catalan-president-calls-for-talks-with-spains-government-after-unrest-quim-torra

CARRERA, Xavier Vilà. 2014. "The domain of Spain: How Likely Is Catalan Independence?", Sage Publications, Inc. URL: http://www.jstor.org/stable/43555055

CONVERSI, Daniele. 1997. *The Basques and Catalans and Spain: Alternative routes to nationalist mobilisation*, London: Hurst

CORDERO, Dani. 2019. "Pro-independence protesters cause travel chaos at Barcelona airport", accessed September 5, 2021. URL: https://english.elpais.com/elpais/2019/10/15/inenglish/1571123222_635456.html

DE LA GRANJA Sainz, Luis, José; NOLLA Anguera, Pere; BERAMENDI G., Justo. 2001. "La España de los nacionalismos y las autonomías", accessed August 22 - 26, 2021. URL: https://dialnet.unirioja.es/servlet/libro?codigo=237385

Editors of ACN Barcelona. 2021. "Between 108,000 and 400,000 attendees in National Day pro-independence rally". URL: https://www.catalannews.com/politics/item/between-108000-and-400000-attendees-in-national-day-pro-independence-rally

Editors of BBC News. 2010. "Catalan protesters rally for greater autonomy in Spain". URL: https://www.bbc.com/news/10588494

Editors of Constitutional Court of Spain. 2014. "Constitutional Short Judgement 42/2014", accessed September 12, 2021. URL: https://www.tribunalconstitucional.es/ResolucionesTraducidas/STC%2042-2014E(2)%20%20DECLARACION%20SOBERANISTA%20%20SIN%20ANTECEDENTES.pdf

Editors of El Mundo. 2003. "Zapatero promete apoyar la reforma del Estatuto de Cataluña propuesta por Maragall", El Mundo. URL: https://www.elmundo.es/elmundo/2003/11/13/espana/1068756801.html

Editors of El País. 2005. "El Parlamento de Cataluña aprueba el nuevo Estatuto". URL: https://elpais.com/elpais/2005/09/30/actualidad/1128068217_850215.html

Editors of Encyclopedia Britannica. 2021. "Spanish Civil War", accessed August 7, 2021. URL: https://www.britannica.com/event/Spanish-Civil-War

Editors of GenCat, n.d. 2021. "The contemporary Government of Catalonia (20th and 21st centuries". URL: https://web.gencat.cat/en/generalitat/historia/generalitat-contemporania/

Editors of GenCat, n.d., "Catalan language". URL: https://llengua.gencat.cat/en/el-catala/origens-i-historia/

Editors of Madrid Embassy, n.d. 2021. "Kingdom of Spain. General Information". URL: https://madrid.embassy.qa/en/kingdom-of-spain/info

Editors of Real Instituto Elcano. 2019. "The independence conflict in Catalonia". URL: http://www.realinstitutoelcano.org/wps/wcm/connect/d8496562-e096-44a1-81da-b871c91ccf62/Catalonia-dossier-elcano-october-2019.pdf?MOD=AJPERES&CACHEID=d8496562-e096-44a1-81da-b871c91ccf62

Editors of Statistical Institute of Catalonia. 2020. "Total and foreign population series". URL: https://www.idescat.cat/poblacioestrangera/?b=0&lang=en

FERNANDEZ MORENO, Luis. 1986. *Decentralization in Britain and Spain: The cases of Scotland and Catalonia*, University of Edinburgh.

FERREIRA, Carles. 2021. "Entrapped in a failing course of action: Explaining the territorial crisis in 2017 Catalonia". URL: https://www.tandfonline.com/doi/full/10.1080/13597566.2021.1907570

FOGUET I BORREU, Francesc. 1966. *Història de la premsa catalana (1966)*. Barcelona: Universitat Autònoma de Barcelona.

HENDERS, J. Susan. 2010. *Territoriality, Asymmetry and Autonomy: Catalonia, Corsica, Hong Kong and Tibet*, United States, Palgrave Macmillan.

HOLODNY, Elena. 2017. "Catalan authorities «have placed themselves outside the law and democracy»". URL: https://www.businessinsider.com/spanish-king-on-catalonia-referendum-in-rare-tv-address-2017-10

KEATING, Michael. 1994. "Naciones, nacionalismos y estados.". Revista internacional de filosofía política. URL: https://dialnet.unirioja.es/servlet/articulo?codigo=2704608

MARTI, David; CETRÀ, Daniel. 2016. "The 2015 Catalan election: a de facto referendum on independence?". URL: https://www.tandfonline.com/doi/abs/10.1080/13597566.2016.1145116?journalCode=frfs20

RIOS, Pere; BAQUERO, S., Camilo. 2019. "Catalan leader condemns violence, calls for meeting with Spain's PM". URL: https://english.elpais.com/elpais/2019/10/22/inenglish/1571754336_234078.html

SOLIS, Fernando, Leon. 2003. *Negotiating Spain and Catalonia Competing Narratives of National Identity*, Bristol, UK: Paperback.

TURP, Daniel; CASPERSEN, Nina; QVORTRUP, Matt; WELP, Yanina. 2017. "The Catalan Independence referendum: An assessment of the process of self-determination". URL: https://www.researchgate.net/publication/321934266_The_Catalan_Independence_referendum_An_assessment_of_the_process_of_self-determination

VILAREGUT, Sáez, Ricard. 2011. "Memory and emergency in Catalan independence. The case of the Platform for the Right to Decide". URL: https://ca.freejournal.org/89952/1/plataforma-pel-dret-de-decidir.html

Centre for Defence and Security Strategic Studies/
"Carol I" National Defence University, December 9-10, 2021

DOI: 10.53477/2668-6511-22-29

THE DEGRADATION OF HUMAN RIGHTS AND FREE PRESS THROUGH THE PEGASUS SOFTWARE IN THE ERA OF SURVEILLANCE, AS A THREAT TO INTERNATIONAL SECURITY. A DEBATE OF CIVIL LIBERTIES AND CENSORSHIP

Maria PÎRVU,
Student, Queen's University Belfast, Belfast, United Kingdom.
E-mail: mpirvu01@qub.ac.uk

Abstract*: The evolution of cyber spying technology presents new and rising dangers; coupled with the easy justification for use of the on-going terrorist crisis these dangers have now become major threats to the international security system. This article aims to provide analysis of these threats, using the new software Pegasus as a focal point of discussion. Developed by the Israeli 'cyber-warfare' company 'NSO', this spyware signals a danger not only to security but freedom of the press and journalistic integrity. This paper's focus will centre on how this software is used for censorship rather than to combat terrorism and will examine the social and political ramifications of said use. As highlight, the case of UAE activist Ahmed Mansoor and his contemporaries who were writing against authoritarian governments will be discussed. This article will urge that strict global legislation is needed to stop the abuse of spyware as a tool of censorship.*

Keywords*: security threat; NSO Pegasus; censorship; citizens' rights; counter-terrorism activism; free press; spyware.*

Introduction

George Orwell's dystopian world of 1984 is famous for the quote "Big Brother is watching you" (Orwell 1949, 3). Although his work has always been considered fiction, the ongoing change of reality proves that we might not be so far from his imaginative world. The spying industry has been merged in the last decades with the world of cyber technology. New alternatives have risen to protect the integrity of the international system, but so have the dangers that could compromise it. Among the most recent ones that surfaced is Pegasus, which was developed by the Israeli company NSO. A powerful and discreet tool, NSO promises that the mission of this spyware is to counter terrorism and crime, however, the recent events reveal that it has been used in other ways as well, some of them being unethical, and potentially illegal.

This article aims to provide a starting point, a warning signal of the rising security issues that Pegasus exemplifies. Through presenting how it operates, examining the threat posed by its advanced technology and distinguishing the main issues that arise from its use, this article becomes a framework for this new potential danger. Specific examples from recent events of potential issues that can arise from its use will be provided for every argument. This article will have a political, legal, and ethical approach on the issue of the Pegasus spyware and will culminate with some recommendations on what should be done in the international system to prevent any security disruption, actions that have already started to happen.

1. Pegasus: an analysis

1.1. What is Pegasus?

The landscape of cyber security is one defined by perpetual evolution, to every new firewall or antiviral software, there is an equivalently new type of malware or backdoor. Due to our modern reliance on technology, cyber threats can fundamentally alter our private and

public safety; these can pose dangers to the individual but have ramifications to the wider world of international security and public liberty. These types of malicious software, like Pegasus, intentionally damage a device or network by penetrating through the internet, email, or text messages, for example hiding under the form of an application, which the victim unknowingly installs. There is a wide variety of malware, such as computer viruses or, in the discussed case, spyware. The Federal Trade Commission (2021) in America defines spyware as "*one type of malware that can monitor or control your computer use*." Once installed in the device, it can be used to monitor the computer's activity, get access to private data and personal information, which can result in fraud commission, identity theft, or the stealth of personal data for various purposes.

The organisation that developed Pegasus is the private Israeli company NSO. In the last decade, this private group has been the focus of international scrutiny. The company describes itself as an ethical organisation that supports government bodies by providing their powerful software in order "to prevent and investigate terror and crime" (NSO Group, 2021), a noble goal. Publicly, their addressing of criticisms levied against that their software has been unethically used is sparse, furthermore, it cannot be found anywhere on the website any information about 'Pegasus', which is their invention, as well as the centre point of the entire scandal, which strengthens scepticism for their true intentions.

The Pegasus software is a spyware trojan that can penetrate any mobile device and access any type of data it owns. It can only be used on mobile smartphone devices and can infect all types of operating systems. It has unlimited access to the target's device and is used to collect all the data a mobile infected possesses. This article will use Amnesty International's (2021) forensic report as a framework on how Pegasus operates. This framework lays out the stages by which Pegasus attacks a device to extract information. The first stage of infection is targeting a device. A link is sent to a smartphone, usually through either SMS or WhatsApp.

From here on, the process remains the same as other software infections, the spyware installs itself and starts accessing everything on the device. Once it penetrates the device all information on it is compromised. It hides as operating systems processes, which makes it much harder to be identified. For example, on the IOS devices, "*most Pegasus process names seem to be simply disguised to appear as legitimate iOS system processes, perhaps to fool forensic investigators inspecting logs.*" (Amnesty International 2021, 27). The final stage is the tracking, as the spyware sends all the data and information accessed on the device to a third party operating in a secret manner that can use it to monitor the victim's life. The information acquired could potentially be used against the target with possibly massive implications to that person and the organisation they are associated with.

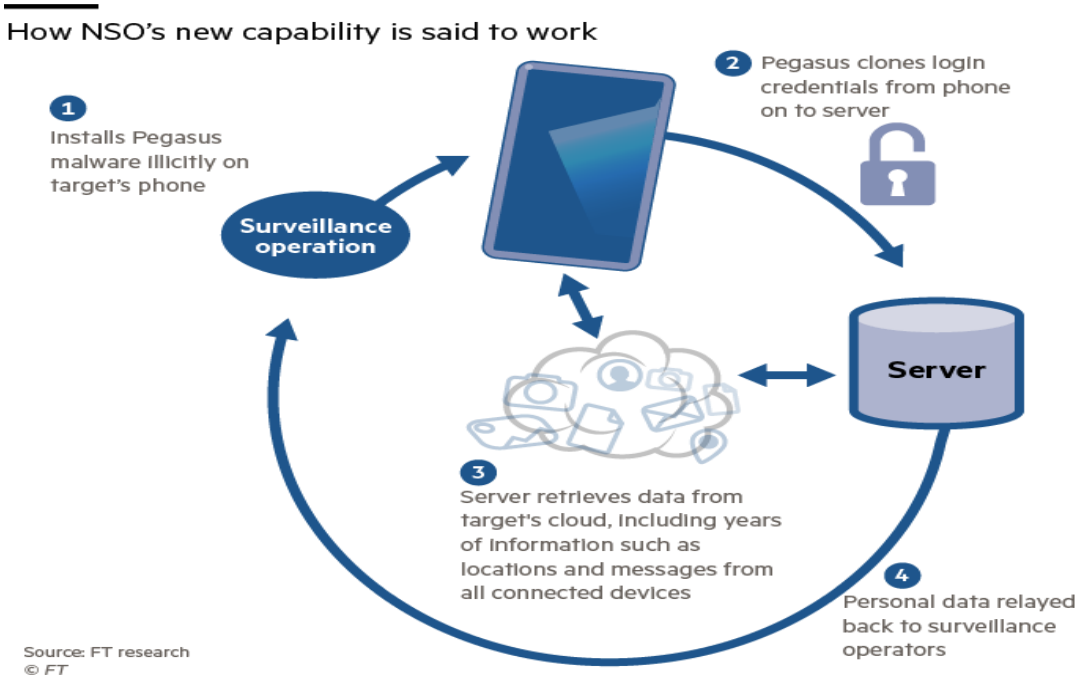

Figure no. 1: Financial Times Research, 2019.

The Pegasus project was created to investigate NSO's actions with Pegasus, and to reveal its abusive use around the world. It is an ongoing international investigative journalism project, initiated by Forbidden Stories (a French media non-profit organisation) and Amnesty International (a non-governmental human rights organization) to conduct forensic analysis over the use of Pegasus. A various number of newspaper agencies, as well as independent journalists around the world, are part of the project and aim to uncover that Pegasus is used not only for its presented purposes. Since 2016, The Pegasus Project unfolded the story of the spyware, identified a leak of more than 50,000 phone numbers that were infected and targeted by the Pegasus software and exposed the use of the spyware in India, Morocco, Italy, Mexico, Saudi Arabia, Hungary, United Arab Emirates and Azerbaijan. Among the phone numbers targeted, human rights activists, leading opposition politicians, lawyers, journalists, and political dissidents were identified. In 85% of the phone numbers targeted, the mobile phones were infected with spyware. (Forbidden Stories, 2021) Their analysis progressively concludes the spyware was used by authoritarian or flawed democratic government bodies to spy on individuals that can be a potential risk to their governance. The investigation will be the starting point for elaborating all arguments in this paper.

1.2. Why is it so dangerous?

This is a powerful tool, but it is especially dangerous for two reasons, firstly the aforementioned 'zero-click' technology and secondly NSO's nature as a non-government private organisation. Immediately Pegasus stands apart from many of its contemporaries as it uses a 'zero-click' technology, which enables it to access the mobile device without the user knowing it at all and leaves no traces of it being on a smartphone. It works by identifying any security breaches and flaws in the operating system or apps and using them to infiltrate the device. This represents a technology that is much harder to track, meaning that it becomes much less detectable to discover. "The technical effort required to identify cases markedly increases, as does the logistical complexity of investigations." (Marczak, Scott-Railton, Al-Jizawi, Anstis, and Deibert, 2020, p. 16). This technology could evolve to a point where it can no longer be identifiable, which leaves devices completely vulnerable to spyware and compromised privacy.

Furthermore, in a similar way to American mercenaries not being reported in war statistics, a government's use of outsourced private spyware does not have to be reported and can remain anonymous and untraceable between the company and the government. Currently, the private sector, particularly corporations, can only be prosecuted under national law by a state if it infringes any human rights. This means that the corporate responsibility for ethical and social issues is left to be self-regulated, which can be a detriment to the transparency and accountability in the private sector. Only sovereign states and other entities that are legally recognized as international actors can be subjected to international law. As a result, government bodies can 'hack' international law, not be held accountable for using this spyware. This lack of accountability could result in human rights abuses, such as the privacy right. There are only just a few international organisations that aim to act as guidance against human rights abuses in the private sector, such as "*United Nations Guiding Principles on Business and Human Rights", "United Nations Guiding Principles on Business and Human Rights, "Company Codes" and "Alien Tort Statute* (Yadav 2020, 370-371). Ultimately, this lack of regulation maintains the privacy of those who might use the spyware. Therefore, when NSO sells the use of its software and it may be used in an abusive manner without accountability, it is easy therefore to see that these principles can be applied to not only domestic surveillance but international ones. Exposing private secrets can have massive political implications and can undermine trust by building an atmosphere of ever-present danger and mistrust, which can culminate in the disruption of international security.

In this way, the existence of software such as Pegasus is a major contributor to the cybersecurity dilemma, which can be a bigger risk to international security. Nicholas C. Rueter (2011) argues that because of the nature of cyberwarfare, the cybersecurity dilemma may be more complicated to overcome than the normal security dilemma. He illustrates the cybersecurity dilemma as a chain reaction of cross-national digital security. A state increasing its digital infrastructure's security by strengthening its defensive or offensive cyberwarfare can lead to the degradation of others. Pegasus creates an unstable atmosphere in the international system. States know that the spyware exists, and other government bodies can use it, which can determine them to strengthen their cyber-security. "*An attacker who does not burrow himself deeply into opponents' cyberspace risks having an empty arsenal when a conflict occurs*." (Kello, 2017) The Pegasus project has revealed that among the leaked phone numbers that were infected with Pegasus, 14 world leaders were identified[1]. It has not been confirmed who coordinated the operations against these world leaders, but if NSO stated that it sells the spyware to governments bodies, it can be deduced that government bodies have used it against these world leaders. This can progressively decrease the mutual trust in the international community, ultimately, the possibility of a conflict may arise.

From an ethical perspective, states who use Pegasus violate the social contract, decreasing the legitimacy of their sovereignty. It is undoubtedly clear that a functioning society is based on the social contract theory, which particularly is the justification of power that law enforcement can exert over the population in exchange for security. Citizens give up some of their freedoms to become a collective secure society governed by the rule of law. Just as John Loke (1689) argues, the power of consent is the most important factor of the social contract. For governments to use the Pegasus spyware for surveillance means that individuals are unable

[1] A.N.: Cyril Ramaphosa (the president of South Africa), Emmanuel Macron (the president of France), Tedros Adhanom Ghebreyesus (WHO's director general), Saad Hariri (former prime-minister of Leabon), Charles Michel (the president of the European Council), Mohammed VI (King of Moroco), Saadeddine Othmani (Moroco's prime-minister), Imran Khan (prime-minister of Pakistan), Felipe Calderón (former president of Mexico) and Robert Malley (American diplomat). For further detail, see (Chrisafis et al. 2021), URL: https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

to assert consent, which, ultimately, leads to governments not being subjected to the rule of law. This can lead to breaches in the social contract, particularly, states not being held accountable for their actions, which can weaken a democratic state. The power of consent is cancelled by the violation of the right to privacy, as "The governors and the governed should be subject to the law." (Taylor 2002, 66).

2. The right to privacy in democratic and authoritarian regimes under the influence of Pegasus

There are many threats the Pegasus spyware imposes to the international security, however, the biggest one and the most investigated one is democracy. By having such a state-of-the-art spyware technology, especially unregulated, governmental bodies in democracies can use it to infringe the human right of privacy or break the fundamentals of democracy.

International human rights law covers the right to privacy in multiple conventions, such as 'International Covenant on Civil and Political Rights (1976, Article 17)', 'Convention on the Rights of the Child (1990, Article 16) International Convention on the Protection of All Migrant Workers and Members of Their Families (1990, Article 14) (United Nations 2021) As highlighted in the universal rights declaration,

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*." (United Nations, 1949, Art. 12)

The use of Pegasus violates all the conventions mentioned above, firstly because it operates a 'zero-click' policy, which does not enable the target to consent at all and represents a new and much more dangerous implication in spyware. This, coupled with the core idea that spyware is an intrusion of the international right to privacy become drivers of how dangerous this new spyware is to the international security.

Not only the use of Pegasus violates one of the most basic human rights, but it can weaken democracies, especially when governments are able to not be held accountable. It can do this by being a contributor to the establishment of various actions over time that can detriment the democracy of a state. An illustration of this argument can be exemplified by the use of Pegasus in Hungary. It has been confirmed that out of the 50,000 leaked phone numbers that were targets of the spyware, Hungarian journalists, media owners and political figures were confirmed victims of Pegasus. (Marczak, Scott-Railton, McKune, Abdul Razzak, and Deibert 2018, 15) The legislation in Hungary allows the government to operate mass surveillance operations on individuals who are not related to any investigations, nor are under suspicion on any law breaches. For this to happen, in the case of an attack of the state's national security, intelligence gathering services can operate without a judicial oversight, without an external assessment, only with the approval and signature of the justice minister. Judit Varga, Hungary's justice minister recently "*has declined to comment on whether the Hungarian government uses Pegasus, but said "every country needs such tools*" (The Guardian, 2021) The justice minister's statement belies a disregard for a fundamental principle of democracy, the separation of the powers of the state. The mere existence of Pegasus spyware in Hungarian journalists, lawyers and opposition politicians is a direct violation to the right of privacy, coupled with the possibility of the government using it become a serious threat to the democracy in Hungary, especially due to its shaken times as a democracy.

Furthermore, authoritarian states can use the spyware to consolidate their regime and to strengthen their control over the population. This added power weakens both the chance of them becoming democratic and the international security. Totalitarian governments are maintained and expand through crushing or discrediting their opposition. In the past, authoritarian governments could have been held accountable for abusing human rights on

political dissidents as there was some physical component, violating the rule of law and being under trial at the Supreme Court in the end. However, the Pegasus software allows authoritarian governments to escape this accountability. NSO is a private company with no obligations to disclose who uses their service. The Citizen Lab's 2018 study revealed examples of authoritarian governments used Pegasus to spy on political dissidents, human rights activists, lawyers, and journalists from 2014 to 2018. This is additional proof that Pegasus can contribute to abuses in the international security.

Table no. 1: Reported cases of individuals targeted with NSO Group's Spyware (Marczak, Scott-Railton, and Deibert 2018, 10)

Country Nexus	Reported cases of individuals targeted	Year(s) in which spyware infection was attempted
Panama	Up to 150 (Source: Univision)[1]	2012-2014
UAE	1 (Source: Citizen Lab)	2016
Mexico	22 (Source: Citizen Lab)	2016
Saudi Arabia	2 (Source: Amnesty, Citizen Lab)	2018

Table 4: Reported cases of individuals targeted with NSO Group's Spyware

Among the individuals targeted by Pegasus, the 51 years old engineer Ahmed Mansoor, appears to be a significant victim, as he is a renowned figure in Middle East and North Africa region, admired for his close implication in human rights activism and criticism of the UEA government. In 2016, he received a text message that claimed to reveal secrets of the tortured prisoners in the UAE if he clicked on the link provided. Ahmed Mansoor forwarded the message to The Citizen Lab and, together with Lookout Security started an investigation. It was concluded that the link contained Pegasus spyware and the operation of attempting to infect his phone was correlated with the UAE Government.

"The attack on Mansoor is further evidence that "lawful intercept" spyware has significant abuse potential, and that some governments cannot resist the temptation to use such tools against political opponents, journalists, and human rights defenders." (Marczak and Scott-Railton 2016, 3).

3. (Not so) free press?

Pegasus becomes an issue of concern in the media world as well, as such spyware is a contributor to the degradation of both free and independent press. Around 180 journalists were targets of NSO Pegasus and the investigations linked different authoritarian governments to the spyware's infection of journalists. (IPI-Admin 2021) Such actions can be a direct infringement of democratic fundamentals, particularly freedom of expression and free and independent press.

The Pegasus spyware is a contributor to the creation of a chilling effect in the international media, as an immediate reaction which, ultimately can lead to censorship of independent media in the long term. The chilling effect can be defined as a "*negative deterrence of communication: that a person or organisation is made physically colder by inhibiting the exercise of their right to free expression*" (Townend 2017, 73) It represents a consorted effort of repression through legal and non-legal means by a regime that aims to limit the exercitations

of the individual's right to free speech. In this context, the acknowledgement and use of the Pegasus spyware can discourage media agencies and journalists to critically engage with governmental actions due to a fear of becoming a victim. It becomes an intimidation tool that can lead to an auto-censorship. Just as the separation of powers regulates the state in a democracy, critical and free media has a significant contribution to influencing government authority over the population. Compromised independent media is not only an infringement of the right to free speech, but also a factor that weakens the quality of a democratic state and strengthens the power in an authoritarian one. In the long term, the use of Pegasus as a tool to create a chilling effect can result in a rise of prominent censorship in the international media. When governments target with the Pegasus spyware independent journalists and media agencies, the process of censorship can happen in a much more discreet manner, which means it can be more effective and efficient.

During their forensic research at Amnesty International, John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2018) revealed that the Pegasus spyware has been repeatedly used on 8 Mexican journalists and, in some cases their family. They highlight that the journalists have been targeted with Pegasus just before or after the killing of a colleague or family member. Just a few days after the murder of Javier Valdez, a Mexican independent journalist, his wife Griselda Triana (who is also a journalist) fell as a victim of the Pegasus spyware, along with another attempt to infect two of his colleagues' phones, Andrés Villarreal, and Ismael Bojórquez. This strategy of targeting close contacts is an illustrator of the rise of the chilling effect through the Pegasus spyware, which can result in journalists auto-censoring themselves due to a fear of becoming victims themselves, or to put their family, friends, and investigations at risk.

4. What should be done?

Because the Pegasus spyware is so dangerous, immediate action needs to be taken. It represents only the beginning in the evolution of incredibly powerful surveillance mechanisms. The first step that needs to be taken to protect the international security is the adoption of a social norm against the Pegasus spyware, which is already happening. Precisely, first, the acknowledgement that the Pegasus spyware is used as a tool to censorship and human rights abuses as well, not only to combat terrorism and crime. Media coverage and public information is needed for this step to be complete. The Pegasus Project became a starting point of media coverage that urges the public to be informed that NSO is a potential threat to the international security. From here, public information can lead to criticism, which can lead to protests against NSO's actions, such as the Protests in Hungary on the 26th of July (Reuters, 2021). This, coupled with Pegasus being a threat to states' security as well, (like government officials being targets) can push the social norm into international consideration and governmental action.

When the social norm against private spyware technology is considered by international organisations it transforms itself into an international norm. This means that governments and international organisations start treating this as a security issue. When this happens, international action can be taken to push back against authoritarianism and for the protection of the rights. Official national investigations need to start to confirm who used the spyware in an abusive manner, so that the truth and clearance can be surfaced. If it will be confirmed that Pegasus was used in unlawful ways, the Israeli government needs to tighten its law around cybersecurity and to held accountable the NSO group for democratic and human rights violation.

If there is enough evidence that NSO's actions were unlawful, international organisations need to urge a change in the international law. The first and most important change in international law is that corporate surveillance companies should be subjected to

international law just like state actors, to ensure NSO can be held accountable for its actions at the International Court of Justice. The international law on espionage currently "either fails to regulate spying or affirmatively permits it" (Deeks, Abebe, Andrias, Cohen, Cordero, Daskal, Kaye, Kendrick 2014, 300) Especially in the cyber espionage area, because international law faces such an impediment, international organisations should encourage states to tighten their national legislations. Before approval, espionage cases should be reviewed and either approved or declined by an independent body within a state. The United Nations Office of High Commissioner (2021) have also urged to the establishment of a global moratorium as an immediate reaction to The Pegasus Project's revelations on the use of surveillance technology until regulations are put in place that follow international human rights standards.

The legislation must also focus on robust notice and consent requirements of spyware by the immediate ban of the 'zero-click' technology. To preserve a secure cyberspace, international organisations should encourage corporate technological companies to use safer ways of encryption, such as the quantic encryption, which is currently almost impossible to be broken.

Conclusion

The spyware technology in the international security world has brough many debates, in terms of its use from an ethical, technological, and political perspective. This article provided an analysis of the rising danger of spyware in the international system, with an emphasis on the Pegasus software developed by NSO. Particularly, how the Pegasus software is different and more dangerous than other tools of spyware and how it affects the international system. By using the information 'The Pegasus Project' provides as a framework, this article argued that the use of this spyware represents a great danger. Firstly, because it becomes a contributor to the process of damaging democracy and simultaneously to the process of strengthening authoritarian regimes around the international scene. Secondly, because it infringes both human rights, like the right to privacy and citizens' rights, like the detriment of freedom of expression by the creation of a chilling effect that promote censorship.

This article laid the groundwork for this new and rising threat and provided an analytical study of the most pressing and dangerous threats this new technology can do. Because this was a starting point of a few of the most dangerous threats Pegasus offers, further elaboration can be done on how NSO's Pegasus can be a contributor to a decrease in a states' security monopoly, which can lead to corporatocracy, about how such spyware can be done in an ethical way, on how the Israeli government should address this issue, or how the impact of Covid-19 digitalisation influenced the evolution of this spyware.

The Pegasus spyware therefore becomes less of a useful help for combating terrorism and crime, but rather a contributor to the unsettlement of the international scene, by contributing to the security dilemma, promoting censorship, and unfairness. Immediate action at a global level needs to be taken, as such technology can shake the global political stage from its core and unpreceded consequences will be seen if no action will be taken. The new challenges of the international technological security world will be increasingly difficult, but so must be the political actors to face them.

BIBLIOGRAPHY:

Amnesty International. 2021. "Forensic Methodology Report: How to Catch NSO Group's Pegasus." Amnesty International. Peter Benenson House, 1 Easton Street London WC1X 0DW, UK: Amnesty International Ltd. Available at: https://www.amnesty.org/en /latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

C. RUETER, Nicholas. 2011. "The Cybersecurity Dilemma." Master Thesis. Department of Political Science in the Graduate School of Duke University. http://docplayer.net/957458-The-cybersecurity-dilemma-nicholas-c-rueter-department-of-political-science-duke-university-date-approved-alexander-downes-supervisor.html

CHRISAFIS, Angelique, Dan SABBAGH, Stephanie KIRCHGAESSNER, and Michael SAFI. 2021. "Emmanuel Macron Identified in Leaked Pegasus Project Data." The Guardian. July 20, 2021. https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

DEEKS, Ashley, Daniel Abebe, Kate Andrias, Harlan Cohen, Carrie Cordero, Jen Daskal, David Kaye, and Leslie Kendrick. 2014. "An International Legal Framework for Surveillance." https://www.ilsa.org/Jessup/Jessup16/Batch%202/DeeksLegal Framework.pdf

Federal Trade Commission. 2021. *Spyware and Malware*. <https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware> [Accessed 8 September 2021]

Financial Times Research. 2019. *How NSO's New Capability Is Said to Work*. https://www.ft.com/content/2f5feb53-e7ff-47b3-ad42-93a8f2bc6aac

Forbidden Stories. 2021. "About the Pegasus Project | Forbidden Stories." Forbiddenstories.org. 2021. https://forbiddenstories.org/about-the-pegasus-project/

General Assembly, United Nations. 1949. *Universal declaration of human rights* (Vol. 3381). Department of State, United States of America.

IPI-Admin. 2021. "Pegasus Project: Full Investigation Needed after 180 Journalists Targeted by Spyware." International Press Institute. July 19, 2021. https://ipi.media/pegasus-project-full-investigation-needed-after-180-journalists-targeted-by-spyware/

KADAM, Munmun, and YADAV Rahul. 2020. "Corporate Accountability and human rights violation". Volume I. Issue II. April 2020.

KELLO, Lucas. 2017. "The Security Dilemma of Cyberspace: Ancient Logic, New Problems." Review of *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*, by Ben Buchanan. https://www.lawfareblog.com/security-dilemma-cyberspace-ancient-logic-new-problems

LOCKE, John. 1689. "Two Treatises of Government". 1st edn. England: Awnsham Churchill. (chapter 2-19)

MARCZAK, Bill, and SCOTT-RAILTON John. 2016. "The Million Dollar Dissident: NSO Group's IPhone Zero-Days Used against a UAE Human Rights Defender."

MARCZAK, Bill, SCOTT-RAILTON John, MCKUNE Sarah, RAZZAK Bahr Abdul, and DEIBERT Ron. 2018. "HIDE and SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." *Citizen Lab Research Report No. 113, University of Toronto*, September.

NARAYAN, Rahul. 2021. "Don't Let Pegasus Convert Citizens into Docile Bodies." *Mint*, June 30, 2021. http://14.139.58.147:8080/jspui/handle/123456789/4078

NSO Group. 2019. “NSO GROUP - Cyber Intelligence for Global Security and Stability.” NSO Group. 2019. https://www.nsogroup.com/

Office of the High Commissioner, United Nations Human Rights. n.d. “OHCHR | International Standards.” Www.ohchr.org. Accessed September 16, 2021. https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx

Office of the High Commissioner, United Nations. 2021. “OHCHR | Spyware Scandal: UN Experts Call for Moratorium on Sale of ‘Life Threatening’ Surveillance Tech.” Www.ohchr.org. August 12, 2021. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E

ORWELL, George. 1949. *1984*. Harlow: Pearson Education.

Reuters. 2021. “Hungarians Protest against Alleged Illegal Surveillance with Pegasus Spyware.” *Reuters*, July 27, 2021, sec. Europe. https://www.reuters.com/world/europe/hungarians-protest-against-alleged-illegal-surveillance-with-pegasus-spyware-2021-07-26/

SCOTT-RAILTON, John, MARCZAK Bill, ANSTIS Siena, RAZZAK Bahr Abdul, CRETE-NISHIHATA Masashi, and, DEIBERT Ron. 2018. “RECKLESS vi Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague.” *The Citizen Lab*. University of Toronto: Citizen Lab Research Report No. 116. https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

TAYLOR, Nick, 2002. State surveillance and the right to privacy. *Surveillance & Society*, *1*(1), pp.66-85.

TOWNEND, Judith, 2017. Freedom of expression and the chilling effect. In *The Routledge Companion to Media and Human Rights* (pp. 73-82). Routledge.

WALKER, Shaun. 2021. “Call for Hungarian Ministers to Resign in Wake of Pegasus Revelations.” The Guardian. July 28, 2021. https://www.theguardian.com/news/2021/jul/28/call-for-hungarian-ministers-to-resign-in-wake-of-pegasus-revelations

DOI: 10.53477/2668-6511-22-30

STRATEGIC SEALIFT CAPABILITIES: THE SPECIAL CASE OF THE UNITED STATES OF AMERICA

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

Abstract*: Along several millennia, sealift capabilities have played a significant role in shaping the political international arena, and the global strategic landscape. We cannot imagine, for example, a fully operational Roman Empire without a massive set of sealift capabilities, able to deploy large armies anywhere around the Mediterranean, and to bring huge amounts of Egyptian grain to Rome. The study is briefly exploring some pivotal moments in global history, when sealift has been massively present; and then it explores, with some details, the present situation of the US strategic sealift capabilities. As far as we know, the ability of the United States to use, in case of need, fully effective strategic sealift is clearly facing important problems and shortages, and this feature of the US national power might generate a lot of problems in many future scenarios, massively impacting strategic evolutions on the World Ocean, in Europe, and mainly in the Asia-Pacific.*

Keywords*: strategic sealift; strategic landscape; US strategic posture; great power competition; strategic forecasting; national power; global capabilities.*

Introduction

Along the past few years, on several occasions, various serious open sources clearly indicated the US strategic sealift capabilities were facing *very* serious problems. And the problems we are talking about *might* be able to seriously jeopardize the general / global strategic capabilities of the United States, in case of major international crises (which are making deployment and use of massive military forces a clear must). In order to better understand such a topic, this study is going to present, first of all, a brief survey of some significant moments in world history when sealift capabilities have been massively important; and then, some data and opinions concerning the present status of the US strategic sealift capabilities, emphasizing the problems they are confronted with, and their consequences.

1. Brief historical survey of strategic sealift and its role

Since Antiquity, almost all great powers (and clearly all *world* powers) had to develop and operate significant *strategic* sealift capabilities, at least moderately successful. The more complex state interests are, and the larger the geographic region a world powers aims to control, the stronger the need for effective *strategic* sealift capabilities becomes. A careful exploration of a significant number of episodes in the world history is strongly illuminating a basic rule that can easily be identified when dealing with strategic sealift: on most occasions we know about, the total number of ships used by a state for missions we can legitimately call strategic sealift is significantly *larger* (and on some occasions *many* times larger) than the number of combat ships operated by the same state, on the same theatre(s) of naval operations. See, for example, the notorious case of the massive strategic offensive of the Persian Empire against Greece, which took place in 480 B.C., ten years after the battle at Marathon. As far as we know – and the text written by Herodotus offers us sufficient details – the enormous Persian military

expedition was logistically supported by a huge number of naval transport ships, while the total number of combat ships securing sea lanes, protecting sea transports and fighting against Greek naval squadrons was clearly smaller. Herodotus wrote that the total number of combat ships (almost 100 % triremes) in the Persian fleet was 1,207, while non-combat (or transport) ships, propelled by oars or sails, some of them specially built to transport horses for the cavalry units, was roughly 3,000 (Herodotus 1964, VII, LXXXIX-XCVII).

Some centuries later, in 204 B.C., at the end of the Second Punic War, "a Roman invasion force of 400 transports carrying 26,000 troops and 1,200 horses and protected by 40 warships crossed from Sicily and invaded North Africa" (Gabriel 2007) – a strategic move directly leading to the defeat of Hannibal at Zama. Later, for many centuries, Rome was the largest city in the entire world, "before London at the time of the Industrial Revolution"; and its total population, most probably more than one million people, "ate a great deal of grain, much of it as wheat" (Kessler and Temin, 2007). In such a situation, really *huge* amounts of grain had to be brought to Rome, mainly by ships, from other regions of the empire, most notably Egypt. And these transports clearly had a major *strategic* importance. It is easy to understand that their uninterrupted success was one of the significant factors explaining the lack of major social unrest, on most occasions, in the very core regions of the Empire. However, to transport, across the Mediterranean, wheat for 1,000,000 inhabitants, *very* many trade ships were needed. It is difficult to accurately estimate their total number, but we can presume that most of them had a quite modest displacement. An encyclopedia of ships, published a few years ago, mentioned that the *average* Roman trade ship might have had, at the zenith of the Empire (at about 300 AD), a total displacement of 80 to 90 tons (Gibbons 2001, 21). Most probably, more than 1,000 such ships could have been necessary to completely cover, uninterruptedly, the wheat consumption of Rome. Some other ships were clearly needed to bring to the harbors of Rome other products consumed by the vast population of the city: olive oil, mainly from North Africa and the Iberian Peninsula, wine, etc. In the era we are talking about, the combat-ready naval squadrons operated by Rome in the Mediterranean, even if very potent ones, clearly had fewer ships (for the general evolution of the Roman *imperial* navy, see Starr 1941) than the commercial ones, used by both the state and private entrepreneurs.

In Late Antiquity (or Early Middle Ages), when the early Byzantine Empire led by Justinian tried to unify again the former imperial provinces around the Mediterranean Sea, Belisarius' expedition to North Africa put in motion several hundred ships, most of them being *transport* ships, not strictly military vessels fit for combat. Dealing with this very episode, modern authors estimate the expedition in 533 A.D. involved roughly 500 sea transport ships, plus 92 combat ships (Paine 2015, 186; Hughes 2009, 76).

The same basic correlation – combat ships are normally fewer than transport ships – can be easily detected on other occasions as well. In *modern times*, for example, this is the situation in many confrontations, within the broader context of the Anglo-Dutch Wars. In February 1653, the Dutch admiral Marten Tromp fought a major battle, three days long, off Portland. He had roughly 70 combat ships, and was escorting a very large convoy, "of two hundred sail" (Mordal 1973, 73-74). Another episode of the same sort took place in June 1693, when the battle off Lagos was fought between a large British squadron, with 23 combat ships, trying to protect a huge convoy with almost 400 ships, and two combined French naval squadrons. One year later, the notorious French privateer Jean Bart, commanding 6 combat ships, attacked a larger English squadron, with 8 large combat ships, guarding a larger convoy of roughly 100 transports, recently captured (Mordal 1973, 112). The same is the situation if we refer to some smaller episodes: on May 11, 1707, "the Chevalier du Forbin sallied forth from Dunkirk at the head of 8 ships… Two days later he came upon a British convoy of 56 merchantmen…escorted by three warships… and a frigate. The French attack was swift and sure" (Mordal 1973, 121). At the

end of the 18th century, on April 8, 1782, the French Admiral de Grasse started a bold attempt to attack and, if possible, conquer Jamaica: he sailed from Martinique "with 35 warships, 6 frigates, and 150 store ships" (Mordal 1973, 151). In the opening stages of the great Anglo-French wars fought after the start of the French Revolution, one of the most relevant episodes we must take into consideration is the set of naval decisions and actions leading to the battle called The Glorious First of June. The French tried to protect, at all costs, a large convoy of 117 transports, carrying badly needed grain from America. The mission was regarded as being *vital* for the national interest, simply because of a "disastrous harvest brought about by political troubles and civil war as much as by bad weather": the convoy, with a clearly significant *strategic* cargo, was protected by 36 warships, 26 of them directly involved in the battle against a British fleet with 26 large combat ships (Mordal 1973, 158-160). A few years later, in the late 1790s, when General Bonaparte sailed to Egypt, his fleet had 33 combat ships (13 ships-of-the-line, 9 frigates, 11 corvettes or lighter ships), and 232 seas transport ships, carrying 32,300 men and 680 horses (Napoleon 1981, 254).

More recently, in the 1920s, the United States prepared several versions of the so-called *War Plan Orange*, a detailed contingency plan to be implemented in case of war against Japan. A detailed work published almost 30 years ago by the US Naval Institute gives us accurate numbers of ships to be used: in the November 1922 plan, built around the hypothesis of an American campaign via Marshalls and the Carolines to the so-called Western base, the total number of major (or large) surface combat ships was going to be 46, while the total number of troop transports, dry cargo and ammunition transport ships, and tankers and colliers was going to be 261 – almost 4.5 times more than that of the large combatants (Miller 1991, 128). The numbers are even more significant if we explore the details of the US Navy plan prepared in January 1925, aimed at establishing a major naval base of operations in the Philippines, which were, at that moment, a territory ruled by the US. This variant of the *War Plan Orange* involved 25 large surface combat ships, 39 troop transports (12 for the USMC, 27 for the army), 83 ships for transporting dry cargo and ammunition, plus 100 oil tankers and 20 colliers (Miller 1991, 128). Again, the sealift component of the plan is – in terms of number of ships – *significantly* larger than the naval *combat* component (25 large surface combat ships, but almost 10 times more sea transport ships: 242, to be more accurate).

The same is the situation if we are talking about most of the Allied convoys used by Western powers, in World War II, to send aid to the USSR, or by the US for transporting war materials to the UK, across the Atlantic. See, for example, the case of convoy *HX 112*, sailing from Halifax to the East, and consisting of 41 cargo ships, escorted by five destroyers and two corvettes (Mordal 1973, 347), or the case of the convoy *HG 76*, sailing from Gibraltar to the UK, in December 1941: 32 merchant ships, escorted by 12 warships - two sloops, two destroyers, seven corvettes, and one aircraft carrier, *HMS Audacity* (Mordal 1973, 348).

In early June 1944, on the occasion of the Allied landing operations on the French coast, in Normandy, a massive number of ships were used: roughly 4,000 transport and landing ships of all sorts, plus some 600 combat ships (Eisenhower 1975, 345). Again, total number of combat ships of all sorts was several times smaller than the total number of transport ships used.

We also strongly underline here that only on *very* few occasions we know about the total number of transport ships is significantly smaller, if compared with that of combat ships acting together with them. One of the earliest (but very clear) examples of this sort is that of the 256 B.C. Roman attempt to invade North Africa, in the context of the Punic Wars: the Roman fleet was made up of roughly 250 combat ships, while the strategic sealift effort (an army of 60,000 soldiers was transported) was made by 80 large sea transport ships (Gabriel, 2007).

2. US strategic sealift capabilities: major realities and trends in recent past

and nowadays

The *recent* history of the US *strategic* sealift capabilities is both very interesting and clearly significant, enabling us to better understand present day realities and trends.

In the opening stages of Worlds War II, for example, even *before* the moment when the huge US shipbuilding program gained full momentum, naval traffic across the Atlantic was clearly impressive, illustrating the vast sealift potential of the US: "on average, there were 120 to 130 cargo vessels on passage every day", in the New York harbor and off Cape Hatteras areas alone (Mordal 1973, 350). Also in World War II, the Western allies (the United States and the UK) sent to the Soviet Union almost 21 *million* tons of aid – weapons of all sorts, ammunition, some raw materials, clothing, industrial equipment, automobiles and several hundred thousand trucks for military use (Beckhusen 2021). Because of obvious geographic reasons, almost all this aid was transported from US and UK ports to Soviet Union (or to Iran, and from there on, on road or rail) by ship, across the Atlantic and the Indian oceans.

In World War II, the size of US naval capabilities of all sorts grew in a really massive way, and in 1952, before the moment when many combat and auxiliary ships got out of active service, the total number of US oceanic combat and auxiliary ships (including transport) that America could use was staggeringly high: 102 airplane carriers, 87 ships of the line and cruisers, 385 destroyers, 207 submarines, plus 530 amphibious ships and 850 other auxiliary ships (Pemsel 1975, 316). Again, total number of transport ships of all sorts was clearly *larger* than the total number of oceanic combat ships.

Starting with World War II, along several decades, the role of US strategic sealift capabilities became more and more important, at *global* level. "In World War II, civilian-crewed US cargo ships controlled by the War Shipping Administration carried about 75 percent of shipments from the United States. The total cargo lifted between December 7, 1941, and the capitulation of Japan was approximately 300.5 million short tons. The US-flag merchant fleet also carried the great majority of military personnel and civilians moving overseas and returning to the United States during and after the war. Approximately 31.5 million measurement tons of supplies were shipped from the United States to the Far East during the Korean War, in the 50's. About 95 percent of these supplies were shipped by sea, with 80 percent carried by privately owned US-flag merchant ships, and 15 percent by Military Sea Transportation Service ships – all crewed by civilian American citizen seafarers. Privately owned US-flag merchant ships delivered 65 percent of the dry cargo shipments to support American forces in Vietnam, and Government-owned ships carried the balance. The Maritime Administration activated 172 World War II era Victory ships from its National Defense Reserve Fleet. Some 15,000 US citizen merchant mariners crewed the vessels. Cargoes totaled more than 85 million measurement tons" (Pike 2000).

Starting with the 1980s, strategic sealift capabilities of the United States grew smaller, step by step, but quite quickly. However, at the zenith of the Cold War, strategic sealift capabilities of the US were *still* very large. A text published by *FAS / Federation of American Scientists* mentioned that "following World War II the primary strategic sealift mission was to rapidly move men and equipment to Europe to defend against a Soviet/Warsaw Pact attack…. sealift would be provided by over 600 NATO merchant vessels and an active U.S. merchant fleet that still numbered 578 major ships as of 1978. Those 578 ships dwindled to 367 over the next 12 years" (Pike, 2000).

The *global* context the US *strategic* sealift capabilities are *now* confronted with is not at all a serene one. On the contrary, neo-imperial and revisionist policies and actions of *both* Russia and China, and the very volatile situation in the Greater Middle East have clear consequences: the United States might be forced to cope, using severely limited sealift

capabilities, with the tremendously difficult task of *concomitantly* operating *both* in the Atlantic-Mediterranean *and* in the Indo-Pacific. In such a situation, at least two problems can be easily identified.

First of all, we are dealing with the *extreme length of potential transportation sea routes*. Even if the Atlantic is not the widest ocean of the planet, distances are significant. There are 2,000 nautical miles between New York and the Panama Canal; and 3,750 miles from New York to the southern tip of Norway; and 3,150 nautical miles between New York and Gibraltar (Chaliand and Rageau 1985, 57). In the Indo-Pacific basin, distances are even more massive: for example, total distance between Los Angeles and Sydney is 6,450 nautical miles (Chaliand and Rageau, 68).

A second problem we are to cope with is the fact that *the ability of even the most important regional allies and other strategic partners of the United States to significantly augment US strategic sealift capabilities is very limited* (*small*, in perfectly blunt terms). In the Indo-Pacific, for example, *Australia*, a traditional strategic partner of the United States (to better understand this, see Australian military contribution in the Korean War, in Vietnam, and more recently in Afghanistan) has to rely, according to official data, on less than half a dozen logistic ships: a governmental White Paper made public a few years ago was listing only one logistics support ship, HMAS *Choules*, plus two *Canberra* Class amphibious ships, and "two new replenishment vessels that will begin service by 2026", plus "a third replenishment vessel or additional logistics support ship" to "be acquired [in] the late 2020s" (*** 2016). A few years ago, according to a piece of analysis published by the Atlantic Council, the strategic sealift capabilities of Japan was very limited as well: it consisted "primarily of three *Osumi*-class amphibious landing ships, each of which can carry 330 troops and 1,400 tons of equipment"; the text we are quoting here from is also offering data enabling the reader to better understand the limits of the Japanese sealift capabilities: "a US heavy brigade combat team (HBCT) consists of about 3,800 soldiers and 20,000 tons of equipment. It would take approximately fifteen days for the SDF's organic sealift assets to transport a US HBCT from Japan to the Korean peninsula, or approximately thirty days to transport a comparable Ground Self-Defense Forces unit to the southern end of the Ryukyu Island chain" (Cliff 2015, 28-29).

The situation is *now* a *very* difficult one, if we are speaking about *allied* capabilities, in the Atlantic *as well*: the US sealift capabilities might be augmented by those operated by the European NATO member states. Now, 11 of these powers in Europe (in strictly alphabetical order: Croatia, Denmark, France, Germany, Hungary, the Netherlands, Norway, Portugal, Slovenia, Turkey and the United Kingdom) are operating, together, the so-called *Sealift Consortium*, which "finances the charter of up to 15 special "roll-on/roll-off" ships", usually called "Ro/Ro, … because equipment can be driven on and off the ships via special doors and ramps into the hold" (***, May 2021). But put together, these 15 ships do have a sealift "total capacity of about 33,700 lane meters ...: three Ro/Ro ships on assured access; residual capacity of five Danish/German ARK Ro/Ro ships on full-time charter; residual capacity of two French Ro/Ro ships; residual capacity of four UK Ro/Ro ships; and one Norwegian Ro/Ro ship on dormant contract" (***, May 2021). At a first glance, almost 34 lane kilometers might be regarded as a very impressive figure, but if we take into consideration the basic fact that just one Stryker brigade has "over 300 Stryker armored vehicles, over 1,200 trucks, utility vehicles, and support equipment" (GAO 2003, 6), we suddenly can more clearly understand one such unit, alone, has to use almost 10 lane kilometers (1,500 vehicles, combat and transport, multiplied by roughly 6 meters each, means at least 9,000 lane meters). So that, the entire sealift capability of the European part of NATO might suffice for transporting less than 4 brigades (which means *less* than two complete divisions). And anyone can easily understand that, *if* Russia is to ever use massive military forces to reshape the balance of power in Western Eurasia, it might easily use significantly *more* airborne, armored, and mechanized units).

In the United States, at this very moment, the most important part of the sealift capabilities (*an important part* of them of a clear *strategic* nature) of the US Navy are provided mainly by the *US Navy's Military Sealift Command* (*MSC*). According to its official webpage, MCS's mission is that of providing "on-time logistics, *strategic sealift* (author's emphasis), as well as specialized missions anywhere in the world, under any condition, 24/7, 365 days a year". The very idea that *strategic* sealift is one of the main jobs this Navy's command is supposed to accomplish in *any* conditions is also underlined by a statement telling us "MSC safely operates, supplies, and maintains the ships that provide logistics support, conduct special missions, move military equipment, supply combat forces, provide humanitarian relief, and *strategically* (author's emphasis) position combat cargo around the world". The same open source already used here indicates the *MSC* is "operating approximately 125 ships daily around the globe" (for all text fragments quoted in this paragraph, see ***, *MSC Mission*).

To better understand the *really major* role of the *US Navy's MSC* in the context of major international conflicts and / or crises, we think it is useful to offer the reader just a few relevant data, concerning the past few decades: "Between 1965 and 1969, MSC transported nearly 54 million tons of combat equipment and supplies and nearly 8 million tons of fuel to Vietnam. MSC ships also transported troops to Vietnam". Later, "during the first Persian Gulf War's Operations Desert Shield and Desert Storm, MSC distinguished itself as the largest source of defense transportation of any nation involved. MSC ships delivered more than 12 million tons of wheeled and tracked vehicles, helicopters, ammunition, dry cargo, fuel and other supplies and equipment during the war. At the height of the war, MSC managed more than 230 government-owned and chartered ships". More recently, the same *MSC* went on playing "a vital and continuing role in contingency operations around the world": "As of January 2013, MSC ships delivered more than 25.7 billion gallons of fuel and moved 126.2 million square feet of combat equipment and supplies to U.S. and coalition forces engaged in operations supporting Iraq and Afghanistan" (for all text fragments quoted in this paragraph, see ***, *History and Heritage*).

MSC is now using 15 large oil tankers "that provide a variety of fuels for ship propulsion, aircraft operations and power generation"; they "are the largest subset of the Navy's Combat Logistics Force (CLF) and also routinely shuttle food and other dry cargo as fleet freight for transfer to customers as their fuel is delivered", and they "provide fuel enabling the fleet to remain at sea and combat ready for extended periods of time" (***, *Fleet Oiler (PM1)*). *MSC* is also using some 20 ships that are elements of the so-called *Special Mission (PM2)* program; these ships "provide operating platforms and services for a wide variety of US military and other US government missions", including "Oceanographic and hydrographic surveys, underwater surveillance, missile tracking, acoustic surveys, and submarine and special warfare support" (***, *Special Mission (PM2)*). Among these ships there are: one cable laying/repair ship; two missile range instrumentation ships; one navigation test support ship; five ocean surveillance ships; six oceanographic survey ships; one sea-based X-band radar; and four submarine and special warfare support ships (***, *Special Mission (PM2)*). We strongly underline that most of the ships belonging to the *Special Mission (PM2)* program *do not* have a direct and / or significant sealift capability (with the notable exception of the four submarine and special warfare support ships, and these have a total displacement which is not made public by the *MSC*). A third important component of the *MSC* is *Prepositioning Force* (*PM3*), with several really large ships, some of them with a total displacement of more than 62,000 tons – see, for example, *USNS Seay*, *USNS Pililaau*, and two other ships, each of them 950 feet long, able to reach a speed of 24 knots and with a displacement of 62,444 tons (***, *Maritime Prepositioning Force*).

Along the past few years, *open sources have clearly indicated the US strategic sealift capabilities are confronted with a set of major problems and weaknesses, significantly eroding the effectiveness of any potential effort of deploying, in case of need, large amounts of manpower and war materiel*. In early October 2018, for example, a very interesting piece of military journalism was stating "with Russia's reemergence as a menace in Europe, the US Army has been laying the foundations to fight once again on the continent it defended through most of the 20th century", but "the US sealift capacity – the ships that would ultimately be used to transport Army equipment from the states to Europe or Asia – is orders of magnitude smaller than it was during World War II. Combine that with the fact that the commercial shipbuilding industry in the US is all but gone, and the US can't launch the kind of massive buildup of logistics ships it undertook during wartime decades ago". According to the author of the text we are here quoting from, in 2018, the US sealift capabilities "available for a large-scale contingency" (major international crises or more or less massive military operations involving deploying and / or supporting major units of the Army to / on other continents) were very limited: no more than "46 ships in the Ready Reserve Force, 15 ships in the Military Sealift Command surge force, and roughly 60 US-flagged commercial ships in the Maritime Security Program available to the military in a crisis". The same text was listing other problems which badly jeopardized the strategic sealift capabilities of the United States: first of all, 24 of the ships belonging to the ready reserve force and to the Military Sealift Command, were steam operated, and "steam is largely obsolete in the commercial world that the US relies upon to keep its emergency stock of trained mariners employed and in seagoing careers"; secondly, most of the senior steam engineers, vital for operating the steam ships, "are in their 50s", and "they're all going to be retiring soon"; and thirdly, the total number of well qualified US citizen mariners "available and willing to sail when required" is low; it might be enough for a very brief major military effort, but "we are about 1,800 mariners short for any kind of long-term sustainment effort", was openly stating Read Admiral (retired) Mark Buzby, a very senior maritime administrator of the US sealift capabilities. (for all fragments quoted in this paragraph, see Larter 2018).

Some months later, in January 2019, *DefenseNews.com.* published a text directly dealing with the worrying general situation of the US sealift capabilities. The text was openly stating the United States sealift fleet "is facing the prospect of an imminent collapse in capacity due to the ships either reaching or exceeding their hull life, according to the US Army"; it was also stating "the most urgent need in the surge sealift fleet is the Ready Reserve Force, a fleet of ships run by the Maritime Administration that are in reduced operating status and spend most of their time in port waiting to be activated in case of a national emergency". According to the data present in the text, new ships are to be needed as early as 2023-2026, and Captain Scot Searles, at that very moment the strategic and theater sealift program manager said, while delivering a brief at the annual US Surface Navy Association's national symposium, "developing the new ships will take anywhere from three to five years", and "in the meantime, the Navy plans to buy used ships off the open market and modify them for use by the Defense Department". The 2019 text we are now dealing with also quoted some fragments from a letter sent, one year before, by the US Army to the US Congress. The letter was a really worrying warning signal, warning the Congress that, "without proactive recapitalization of the Organic Surge Sealift Fleet, the Army will face unacceptable risk in force projection capability beginning in 2024"; it also stated "by 2034, 70% of the organic [sealift] fleet will be over 60 years old - well past its economic useful life; further degrading the Army's ability to deploy forces", and "shortfalls in sealift capacity undermine the effectiveness of US conventional deterrence as even a fully-resourced and trained force has limited deterrent value if an adversary believes they can achieve their strategic objective in the window of opportunity before

American land forces arrive" (for all data and fragments quoted in this paragraph see Larter January 2019).

Several months later, in September 2019, the *US Transportation Command* (*TRANSCOM*) has "ordered the largest stress test of its wartime sealift fleet in the command's history, with 33 out of 61 government-owned ships being activated simultaneously", and "the results were bad, according to a new report", *DefenseNews* was reporting on December 31, 2019. The text we are quoting here from explains "in a crisis, nearly 90 percent of all Army and Marine Corps equipment would be carried by ship", but at that moment of the stress test we are speaking about, an astonishing low – and really worrying – percentage of the ships involved were really fit for their role: "overall, 40.7 percent of the 61 ships operated by Military Sealift Command and the Maritime Administration were fully ready to support a major sealift operation". More than this, 22 of the 61 ships which were directly involved in the 2019 wartime sealift stress test were not at all fit for the job to be done; a naval specialist said "you had 22 out of the 61 ships in either C-5 or C-4 condition… C-5 means that you can't even leave the dock; C-4 means you can leave the dock but you are not in any condition to sail any real distance. In my ballpark, that's non-mission capable". The same specialist, now a university professor at Campbell University, has also stated that 9 of the 33 ships specially and temporarily activated for the 2019 sealift stress test "had issues", and "three of them were C-4 level" (for all fragments quoted in this paragraph, Larter December 2019).

One year later, in 2020, two senior officials in the Pentagon have delivered an even more somber evaluation of the problems the US strategic sealift capabilities might be confronted with, in case of a major international crisis. In March 2020, Army General Steve Lyons, at that moment the acting commander of the US Transcom (Transportation Command) testified at a joint hearing of both the House Armed Services Committee's Subcommittees for Seapower and Projection Forces, and Readiness. He stated, on that very occasion, "today, I am confident in our ability to successfully execute our mission, but the risk is increasing", and the official media text we are quoting here from explains the General was openly "referring to the insufficient quantity and aging fleets of sealift vessels and aerial refueling tankers". On the same occasion, Mark H. Buzby, at that time the acting maritime administrator at the *US Maritime Administration* (*MARAD*), a structure operating the naval vessels that are a part of the *US TRANSCOM* (Transportation Command), has said "this is an efficient and effective force for moving cargoes worldwide during peacetime… [but] I'm concerned about its ability to reliably project and sustain power globally in a contested environment. To address this, we must strengthen our sealift capability and reverse declines in the US-flagged commercial fleet and US shipbuilding and repair industry" (for all the fragments quoted in this paragraph, Vergun 2020).

In July 2021, *The Maritime Executive* has published a piece of news presenting the most recent data used in this text, enabling us to understand how serious the problems of the US sealift capabilities can be. According to the article, "neglect over the last decades has seen this pillar of US military strength begin to crack", and Army General Stephen R. Lyons, "our sealift fleet is able to generate only 65 percent of our required capacity, and is rapidly approaching the end of [its] useful life". More than this, Rear admiral Buzby, a former senior official of *MARAD* (Maritime Administration), was stating "the Merchant Marine is at least 1,800 officers short of what would be necessary in wartime" (for all text fragments quoted in this paragraph, see Brown 2021).

Another *massively significant* problem US strategic sealift capabilities are confronted with are the increased risks generated by the more and more robust presence, in the Atlantic, of the nuclear-propelled Russian submarines. In September 2021, *Military Times* published two interesting texts directly dealing with this problem. One of them underlines "Navy leaders have

cautioned about increased Russian undersea activity in the Atlantic Ocean", a reality leading to the resurrection of the US 2nd fleet, in direct "response to greater levels of Russian activity in the North Atlantic and Arctic, including undersea" (Stancy Correll 2021). The other one is openly stating "the Navy is organizing East Coast destroyers to better protect the homeland from Russian threats – specifically those undersea – as part of a new initiative called Task Group Greyhound" – at this very moment two large destroyers are directly belonging to an ad-hoc task group, and this naval group "will grow to include The Sullivans, which will replace Donald Cook when that DDG goes into maintenance, as well as Cole and Gravely next year to create a four-ship force that can have two ships ready for a mission on short notice" (Stancy Correll and Eckstein 2021). A supplementary discussion on the way in which two (or even four) destroyers might be regarded as a fully adequate force for patrolling (and defending) the entire North Atlantic might be very useful, but it clearly goes beyond the already listed goals of the present study.

Brief conclusions

Along the past few decades, the US strategic sealift capabilities grew smaller and smaller (if we are speaking about the total number of available ships). Nevertheless, the general context on the international arena is more and more volatile, and more and more dangerous. In such a situation, the basic conclusion of this study is that using fewer and fewer material resources (some of them overaged and / or almost obsolete), and not fully adequate manpower resources, the US *strategic* sealift capabilities might face *huge* problems in different situations – *mainly* if confronted with the perfectly possible task of having to cope, for example, with two (or more) *concomitant* major international crises. Most probably, the most optimistic future scenario we might design is one in which, quite soon, the US strategic sealift capabilities are going to be massively augmented (new ships, new training programs, new massive budgetary allocations). However, according to what we know at this very moment, from all sorts of reliable open sources, real chances for such an outcome are really, really *very* slim.

BIBLIOGRAPHY:

***. 2016. "Air and Sea Lift Capability". 2016. *2016 Defence White Paper*, https://www.defence.gov.au/Whitepaper/docs/Air-Sea-Lift.pdf

***. n.d. "Fleet Oiler (PM1)". Date not indicated (n.d.). Official webpage of *U.S. Navy's Military Sealift Command* (https://www.msc.usff.navy.mil/). https://www.msc.usff.navy.mil/Ships/Fleet-Oiler-PM1/

***. n.d. "History and Heritage". Official webpage of *U.S. Navy's Military Sealift Command* (https://www.msc.usff.navy.mil/). n.d. https://www.msc.usff.navy.mil/About-Us/History-and-Heritage/

***. n.d. "Maritime Prepositioning Force". Official webpage of *U.S. Navy's Military Sealift Command* (https://www.msc.usff.navy.mil/). n.d. https://www.msc.usff.navy.mil/Ships/Ship-Inventory/Maritime-Prepositioning-Force/

***. n.d. "MSC Mission". Official webpage of *U.S. Navy's Military Sealift Command* (https://www.msc.usff.navy.mil/). n.d. https://www.msc.usff.navy.mil/About-Us/Mission/

***. May 2021. "Strategic Sealift". Official *NATO* webpage. Last updated May 12, 2021. https://www.nato.int/cps/en/natohq/topics_50104.htm

BECKHUSEN, Robert. 2021. "The Secret Way the Allies Won World War II". *The National Interest*, April 3, 2021. https://nationalinterest.org/blog/reboot/secret-way-allies-won-world-war-ii-181804

BROWN, Geoffrey. 2021. "U.S. Strategic Sealift's Merchant Mariner Problem". *The Maritime Executive*, July 2, 2021. https://www.maritime-executive.com/editorials/u-s-strategic-sealift-s-merchant-mariner-problem

CHALIAND, Gerard, and RAGEAU, Jean-Pierre. 1985. *Strategic Atlas. A comparative Geopolitics of the World's Powers*. New York: Harper & Row, Publishers, Inc.

CLIFF, Roger. 2015. "Japan's Security Role and Capabilities in The 2020s. Japan as a Regional Security Leader", *Atlantic Council. Brent Scowcroft Center on International Security*, November 2015. https://www.files.ethz.ch/isn/194920/Japan_s_Security_Role.pdf

EISENHOWER, Dwight D. 1975. *Cruciadă în Europa* [*Crusade in Europe*]. București: Editura Politică.

GABRIEL, Richard. 2007. "The Roman Navy: Masters of the Mediterranean", *historynet.com*, post December 2007 (in December 2007, the text was firstly published in *Military History* Magazine). https://www.historynet.com/the-roman-navy-masters-of-the-mediterranean.htm.

GAO. 2003. "Military Transformation: Realistic Deployment Timelines Needed for Army Stryker Brigades. June 30, 2003, *GAO-03-801 Report to Congressional Committees*, https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-03-801/html/GAOREPORTS-GAO-03-801.htm

GIBBONS, Tony (general editor). 2001. *The Encyclopedia of ships*. Enderby, Leicester: Silverdale Books.

HERODOT [Herodotus]. 1964. *Istorii* [*Histories*], vol. II, București: Editura Științifică.

HUGHES, Ian. 2009. *Belisarius: the last Roman general*. Yardley, Pennsylvania: Westholme Publishing, LLC.

KESSLER, David, and Temin, Peter. 2007. "The organization of the grain trade in the early Roman Empire", in *Economic History Review*, 60, 2: 313-332. https://www.jstor.org/stable/4502066

LARTER, David B. 2018. "The US Army is preparing to fight in Europe, but can it even get there?". *DefenseNews.com*, October 8, 2018. https://www.defensenews.com/naval/2018/10/08/the-army-is-preparing-to-fight-in-europe-but-can-it-even-get-there/

LARTER, David B. January 2019. "Facing a sealift capacity collapse, the Navy seeks strategy for new auxiliary ships". *DefenseNews.com*, January 16, 2019. https://www.defensenews.com/naval/2019/01/16/facing-a-sealift-capacity-collapse-the-navy-hones-in-on-a-strategy-for-new-auxiliary-ships/

LARTER, David B. December 2019. "The US military ran the largest stress test of its sealift fleet in years. It's in big trouble.". *DefenseNews.com*, December 31, 2019. https://www.defensenews.com/naval/2019/12/31/the-us-military-ran-the-largest-stress-test-of-its-sealift-fleet-in-years-its-in-big-trouble/

MILLER, Edward S. 1991. *War Plan Orange: the U.S. strategy to defeat Japan, 1897-1945*. Annapolis, Maryland: Naval Institute Press.

MORDAL, Jacques. 1973. *Twenty-five centuries of sea warfare*, London: Abbey Library.

NAPOLEON. 1981. *Memorii* [*Memoirs*], vol. I. București: Editura Militară.

PAINE, Lincoln. 2015. *Marea și civilizația: o istorie maritimă a lumii* [*The Sea and Civilization. A Maritime History of the World*]. Iași, București: Editura Polirom.

PEMSEL, Helmut. 1975. *Von Salamis bis Okinawa. Eine Chronik zur Seekriegsgeschichte*. Munchen: J.F. Lehmanns Verlag.

PIKE, John. 2000. "Sealift". *Federation of American Scientists*, text updated October 19, 2000. https://fas.org/man/dod-101/sys/ship/sealift.htm

STANCY Correll, Diana. 2021. "A 'persistent, proximate threat': Why the Navy is preparing for a fight under the sea". *Military Times*, September 10, 2021. https://www.militarytimes.com/news/your-navy/2021/09/10/a-persistent-proximate-threat-why-the-navy-is-preparing-for-a-fight-under-the-sea/

STANCY Correll, Diana and ECKSTEIN, Megan. 2021. "New US Navy task group taps destroyers to focus on countering Russian undersea threat". Military Times, September 27, 2021. https://www.militarytimes.com/news/your-navy/2021/09/27/new-us-navy-task-group-taps-destroyers-to-focus-on-countering-russian-undersea-threat/

STARR, Chester G, Jr. 1941. *The Roman Imperial Navy 31 B.C. – A.D. 324*. Ithaca, New York: Cornell University Press.

VERGUN, David, DoD News. 2020. "Low Supply, Old Ships Put Sealift at Risk, DOD Officials Say". U.S. *Department of Defense (DoD) News*, March 12, 2020. https://www.defense.gov/Explore/News/Article/Article/2110444/low-supply-old-ships-put-sealift-at-risk-dod-officials-say/

DOI: 10.53477/2668-6511-22-31

SEARCHING FOR POLITICAL EFFECTIVENESS: THE STRATEGIES BEHIND THE MILITARY UNIFICATION OF JAPAN

Ioana-Flavia DRĂGOIANU,
Bachelor's degree student, Security Studies, Faculty of Political Science,
University of Bucharest, Romania.
E-mail: flaviadragoianu@yahoo.com

Abstract: *Over the course of millennia power laid in the hands of generals and rulers and their ability to act – but so did their downfalls. Thus, the first part of this presentation will be focused on the importance of strategy and tactics in any kind of rule. Furthermore, Japanese warfare will be anatomized – how the samurai became elite warriors, weaponry, the transition of samurai warfare during the Sengoku Period and its importance to the fight for supremacy between the Japanese Clans. The goal of this paper is to unravel the conundrums of The Age of War from a political frame of reference, under three powerful influences – Oda Nobunaga, Toyotomi Hideyoshi and Tokugawa Ieyasu. The discussion will then shift towards analyzing the impetus that put in motion their plans and the ways they achieved power, their brilliant strategies and their undoing, whilst using the knowledge regarding Political Science and International Relations to determine the political legacy of their actions.*

Keywords: *Sengoku Period; strategy; subterfuge; warfare.*

Introduction

In a competition, strategy is the only aspect differentiating those who succeed and those who do not. In a rivalry-filled contention, the winner takes it all and the one who is vanquished suffers the loss of land, title and renown. In order to do so, being a master of the battlefield is a must.

One of the important factors in one's supremacy over another is adapting both the tactics and the warfare. Thus, we shall delve into Japanese warfare. Firstly, the Samurai will be the first towards which our focus will shift. The word Samurai comes from the Japanese verb saburau, which means "to serve" and it was initially used to refer to servants. Only in the 8th century it starts encompassing a military implication. *The nature of the samurai ensured that the history of samurai warfare involves two very important aspects: the military activities of the group, through strategy and tactics, and the military prowess of the individual warrior.* (Turnbull, 1996, 10) The samurai become an important factor in analyzing the political Unification of Japan because the Sengoku period brought a change observable only through the bond of loyalty.

Loyalty, both to the Shogun[1] and the daimyo[2] is expressed through a neo-Confucian concept called *taigi – meibun*. *Taigi* refers to the duty owed to the one above you and *meibum* is the moral imperative in the relationship the sense of duty creates. (Steben, 2002, 136) It is the perfect description between a benevolent lord and his loyal subjects. Following the "way of the warrior" was a matter of honor, superior morality and lifestyle, which propelled the Samurai to the top of the warrior class, being considered part of the elite. Many also chose to commit suicide to follow their lords even in death.

[1] A.N.: Hailing from families of esteemed ancestry, a shogun was appointed by the emperor and ruled the country
[2] A.N.: Daimyos were feudal lords that ruled over their respective clan's land.

1. The breaking point towards the age of warring states

The corrosion of Japan's stability started during the Ashikaga Period (Ashikaga *Bakufu*, 1336-1573) due to regionalization and the provincial's lords struggle for autonomy. *Their disinterest in and inability with regard to state administration, the weakening of the shōen system*[3] *and the inheritance disputes that arose over land and property contributed to this process*. (Culeddu, 2018, 90) By the 16th century, the Ashikaga *Bakufu* was losing control, resulting in endemic civil wars. The loss of the authority of a central power to quell the fires of conflict led to chaos in Japan and to a period that remains known under the name of Sengoku Jidai, or the Era of Warring States (1573-1603)

The story of this period is one of careful planning, hidden deals, self-interest, bold action and, of course, massive bloodshed. (Andressen, 2002, 60) During the Sengoku Period (1467-1615) power was thrust in the hands of hundreds of warlords, or daimyo - some more covetous than others, but not all capable of fully attaining ultimate influence over the others. Each daimyo was in charge of his own territory, called a domain and each domain belonged to a clan (Uji), thus, making alliances became an important way of maintaining power and influence.

Further, we shall discuss the ascent to power of three most prevalent daimyo of the Era of Warring States, their downfalls and the focal point of their political legacy – the Unification of Japan – by presenting their way of thinking and the strategies they chose in dire situations through their most significant actions and battles.

2. The Strategy of Unification

The art of war is of vital importance to the State. It is a matter of life and death, a road either to safety or to ruin. (Sun Tzu, 2000, 3) Such was the case in 16th century Japan, where struggle for power overcame the country. In this time, three daimyos distinguished themselves from the others through their resolve, ingenuity and strategies, but also through their contrasting approaches, better expressed through an old Japanese anecdote: Encountering a cuckoo that would not sing, Nobunaga said he would kill it, Hideyoshi said he would persuade it to sing, and Ieyasu would wait for it to sing. (Cortazzi, 1991, 121) This shows how the traits that helped them rise above other daimyo and remain ingrained in the history of Unification.

Oda Nobunaga: the man who mixed the dough

Oda Nobunaga is known as a brilliant but ruthless tactician, capable of learning from his mistakes and adapting to any situation. *He was the ultimate warlord, without peer when it came to brutality and self-interest*. (Henshall, 2012, 46) After the death of Oda Nobuhide, the Oda family enters into a crisis, as the relatively small size of the clan makes them an easy target to the bigger, more powerful clans. Hence, it comes as a surprise that he names Oda Nobunaga his heir in 1551 – especially since he was not well-liked due to his temper and non-traditional approach, some even committing seppuku as an act of revolt towards his newly acquired title. Despite this, he can also be considered an insurgent, his revolutionary outlook differentiating him in a chaotic and conventional state.

One of the first particularities we notice is his acumen, being capable of making good and strategic calls. We notice this during his war with Nobukata, his cousin, for the rest of the Owari province. Wanting to ultimately secure his position as daimyo, he recruits commoners and trains them, with the purpose of matching Nobukata's army in numbers and attacking – and

[3] A.N.: An important element in medieval Japan's economy, the shōen system was focused on private ownership of estates, which were exempted from paying taxes. They became, in a way, a separate political and military power, whilst also forming alliances to further consolidate power.

he succeeds in doing so, rooting his decision on the Japanese notion of *On* which refers to repaying a favor received (Culeddu 2008, 195) This guarantees the full potential of the commoners he now marches to war.

His innovative approach is accentuated during the Battle of Ukino (1558), when he fundamentally changes the Japanese type of warfare. In 1543, Portuguese cargo shipwrecks in Japan and comes ashore on the island of Tanegashima south of Kagoshima (Hall, 1991, 1), leading to the first introduction of firearms in Japan. The issue was, however, a slow reloading time, the possibility of malfunctioning, the recoil and the abundance of smoke, which made them quite unappealing to some. (Turnbull, 1996, 74) But to Nobunaga, the Portuguese Arquebus becomes the key to victory. He buys a large quantity of firearms and creates a killing zone, leading Nobukata's soldiers to their demise. It is interesting to analyze how is it that Nobunaga's army wins, despite being less prepared in the art of battle. Samurai were trained soldiers, hardened by continuous war for hundreds of years. Despite this, the commoners, or *Ashigaru*, were driven by their need to acquire more. Simply put it – they didn't have much to begin with, but their recruitment in the warring ranks gave them a purpose and the possibility to gain more. And that is exactly what turned them into such a lethal force.

This is one of the crucial moments in Oda Nobunaga's life. He, in a way, earns legitimacy in the grander scheme of the warring lords, especially as the sole ruler of the Owari Province. But in 1560, his goals clash with Imagawa Yashimoto's ones, who wanted to seize the heart of the state. Claiming the capital, Kyoto, was an ambition amidst the daimyo - being the center of power of Japan, conquering it would mean uniting all the daimyo under a single, centralized power. This action puts the basis of one of the most important battle for Oda's strategic thinking and cunningness – the Battle of Okehazama, regarded as one of the *greatest combats in the world.* (Brinkley, 1915, 478)

Imagawa Yashimoto's entrance in Owari seemes promising, as he manages to attack and capture some of Nobunaga's fortresses. Having such a large army at hand, he divides it in groups in order to cover more land, an action that ultimately seals his fate. Realizing that he is heavily overwhelmed, Imagawa's army outnumbering him 12 to 1 (Turnbull, 2002, 42), Nobunaga decides to outwit his opponent. Hence, he prepares a surprise attack, knowing that larger troops can be also a disadvantage to the lord – cut the head that holds them together, and they will be too disoriented and stunned to fight back. Without orders, the troops would scatter, not able to communicate to the daimyo to plan an attack *Most fortunately for the Owari troops, their movements were shrouded by a heavy rainfall, and they succeeded in inflicting serious loss on the invading army, driving it péle-mêle across the border and killing its commander-in-chief, Yoshimoto.* (Brinkley, 1915, 478) The battle's importance is also amplified due to the fact that two of the most important people in the history of the Unification of Japan collide, forming an alliance – Oda Nobunaga and Tokugawa Ieyasu, the late Imagawa's general.

Further, Owari Province's daimyo continues with his victories, seemingly becoming more and more ruthless in his mission to seize the capital and subsequent power this action would bring. In 1568 he manages to capture Kyoto, but he faces opposition of both daimyos (Asai and the Asakura families) and the Ikko-Ikki buddhist sect, while the threat of peasant rebellion looms over his head. (Turnbull, 2002, 43-44) However, he deems the Ikko-ikki as the more pressing issue on account of being the cause of many uprisings and having a general displeasure towards daimyo, realizing that *political independence of the Buddhist sects stood between him and national domination.* (Maison & Caiger, 1997, 175)

He reveals his controversial and relentless character even more during his attack on the monks of Mount Hiei in 1571. *This was probably the only military action of Nobunaga's career so controversial that even some of his own generals opposed the move, but it happened nonetheless.* (Turnbull, 2002, 44) Mount Hiei has been generally appreciated as a place of peace

of holy origins, warding out the evil. But, because of the alliance the monks made with the Ikko-ikki, they became a deterrent aimed towards anyone who dares oppose him. Despite the clear warning, this action also enraged the other daimyo and made Nobunaga a target even more than before.

Despite his forceful approach, Nobunaga attended civil affairs and build better castles (more detail here). He gradually started gaining control of the country through under the apothegm inscribed on his personal seal – Tenka Fubu, meaning "A Unified Realm under Military Rule" (Henshall, 2012, 47) He only achieved half of his goal when he was assassinated by one of his generals in 1582.

3. Toyotomi Hideyoshi: the man who baked the cake

Toyotomi Hideyoshi, despite his humble origins, rose to hold Oda Nobunaga's place after his death. *He was a self-made man, a peasant foot-soldier's son who rose through the ranks to become one of Nobunaga's most capable generals. Perhaps most importantly, Hideyoshi was known as a brilliant leader, able to win friends and forge alliances to avoid needless bloodshed, yet he could fight ruthlessly when necessary.* (Andressen, 2002, 61)

Although he took any occasion to form alliances, avoiding bloodshed when needed, his strategic prominence is highlighted by the battles he did fight. One of the first issues that arise after his coup (having seized power from the heirs Nobunaga named) was his war with Shibata Katsuie and Sakuma Morimasa in 1583. During this battle, Shizugatake castle had become a nodal point between the two rival sides, particularly because it was the last one standing. Sakuma Morimasa's mission was to siege it and break down the barrier the three castles represented -However, Hideyoshi unexpectedly attacks, winning the Battle of Shizugatake. (Brinkley, 1915, 495) This victory ensures his role as Nobunaga's successor, making him the *de facto* ruler of Japan.

One of the threats he encounters in his stature of power was Tokugawa Ieyasu, with whom he had to form an alliance, which he manages to do by marrying his sister with Ieyasu, exchanging hostages and offering him a pledge of alliance. (Mason, 1997, 47) The hostage system is once again proof of Hideyoshi's --- thinking. Two hostages are to be exchanged, both of them of great importance. For instance, Tokugawa gave Hideyoshi his second son, while the latter offered his mother. (Henshall, 2012, 48) This ensured that the alliance would not be broken, as the hostages would be executed.

The sole reason for Toyotomi's relative smooth ascent was the fact that one of the major set-backs he had was solved – his origins. Nobunaga might not have had an extremely remarkable bloodline, but he was a small-scale daimyo. On the other hand, Toyotomy Hideyoshi was a peasant warrior, an Ashigaru - and that makes the titles he acquired during his lifetime even more momentous. Consequently, *in 1585 he had himself adopted by Konoe Sakihisa, who could boast of the most exalted lineage within the Fujiwara line*, (Hall, 1991, 46)

After fully gaining the power, Hideyoshi sets his sight on the political and social scene, trying to establish a sense of order and stopping daimyo and commoners alike from rebelling. If Nobunaga's way of doing so was dominating the world through weapons, Toyotomi used subterfuge and tactical decisions. In contrast, Nobunaga's time can be considered one of military consolidation and the time following Toyotomi's coming of power one of institutional changes.

One such important decision is the *kunigae* (province-change technique). He would send vassals, whose loyalty he would question in remote areas in order to burn their power from the roots, whilst the loyal would be held closer to him, in the epicenter of their potential. It was especially easy to do so due to the fief redistribution strategy, which consisted in seizing the land of the opposing daimyo and redistributing it to those loyal as a reward. (Andressen, 2002, 62)

Acknowledging the threat of the now-armed peasants left behind, he enforced the "Sword Hunt" in 1588, during which peasants were forced to give up their armor and swords.

(Mason, 1997, 78) By restricting their access to weapons, they could quell an uprising before it even began.

After gaining control of almost all of Japan, Hideyoshi is left with only two threats: Date Masamune and Hojo Ujimasa, for they did not proclaim their allegiance. (Brinkley, 1915, 495) After the Hojo clan exhibits a hostile attitude towards Hideyoshi, *he employed the familiar tactic of surrounding the castle with an overwhelming force and waiting for the inevitable surrender* (Mason, 1997, 177) which comes in July 1590. When Date Masamune learns of the Hojo Ujimasa's loss, he realizes he is the only one standing between Hideyoshi and his control over Japan, therefore he decides to comply to the daimyo's rule and terms. *Thus, for the first time since the middle of the fifteenth century, the whole empire was pacified.* (Brinkley, 1915, 504)

Having Unified Japan under his rule, during the 1590s Toyotomi Hideyoshi aims at an even bigger goal, planning on attacking China and Korea – nonetheless, although he manages to weaken the first and destroy certain parts of the latter, but he never manages to create an empire.

Before dying due to sickness in 1598, he names his son, Hideyori, as his heir and implements a Court of Regents to make sure history does not repeat itself. *Given the tradition of centuries of scheming and treachery among leaders vying for power, however, it comes as no surprise that the structure Hideyoshi left in place did not last long after his death in 1598.* (Andressen, 2002, 64)

At the end, *"Peace" was the slogan that Hideyoshi carried with him as he unified the country* (Hall, 1991, 47), setting up the locus for Tokugawa Ieyasu's rise to power as Shogun.

4. Tokugawa Ieyasu: The Man Who Ate the Cake

Unlike his predecessors, *Tokugawa boasted of descent from the Minamoto clan* (Culeddu, 2013, 68), meaning he could be appointed Shogun. Despite being part of the Court of Regents selected by Hideyoshi, Tokugawa disputes the matter of the succession, wanting to gain the power for himself – but in the process, the other daimyo turn against him because of their fear of Tokugawa's power and legitimacy. One such warlord was Ishida Mitsunari, who in 1600 attacks Ieyasu's forces at Sekigahara. Ieyasu mobilizes his and his allies' forces, and plans to attack Ishida's ally, Uesugi, from five different directions, having a total of 75 000 men under his command. (Brinkley, 1915, 560) After the outnumbered forces of the Ishida's coalition scatter, Tokugawa Ieyasu at last has no threats left and can start consolidating his road to the ultimate goal – becoming shogun. The Battle of Sekigahara ended the Era of Warring States and marked the beginning of Tokugawa's hegemony, *which gave rise to a highly centralized power structure, capable of exerting nationwide enforcement over military and fiscal institutions.* (Hall, 1991, 4)

It takes him three years to finally ascend to the throne, and, in 1605, he passes the title to his son, while he keeps making decisions unofficially. After over a century, *the shogunate itself, the government of the Tokugawa hegemony, gave form to the "Great Peace" that was to last until well into the nineteenth century.* (Hall, 1991, 1)

Conclusions

The struggle for maintaining, and later acquiring power during a near continuous state of decentralization and civil war is an interesting matter, as it brings unexpected turns and high-stakes. Hence, we saw how in a "daimyo phenomenon" (Hall, 1991, 1) dominated state three great warlords stood out from the rest through their brilliant strategies and callousness, perseverance and machinations and at the end, forbearing attitude and consistency.

The Sengoku Jidai revealed a weakened Japan, that was prone to crumbling in the face of any threat. The power void was filled. In the research article *The Antecedents of*

Deinstitutionalization, Christine Oliver considers deinstitutionalization as involving three processes: dissipation, rejection or replacement, which refer to the outcome of the vacuum of power left behind. It can either dissipate (thus stop existing altogether), the rule can be rejected or it can be replaced by a more proficient one. We see that Japan follows the latter process, rebuilding itself on the stability the three successive daimyos attained.

Ultimately, we not only see a period of unending bloodshed and cruelty, *but a period that began with wars fought with bow and arrow from wooden stockades and ended with stone castles bombarded with cannons. It was an age that began with an isolated Japan where the wars of continental East Asia had little influence, and ended with a Japan that traded with Europe and sent mercenaries to fight abroad* (Turnbull, 2002, 14)

BIBLIOGRAPHY:

ANDRESSEN, Curtis. 2002. *A short history of Japan: From Samurai to Sony*, Allen & Unwin.

BRINKLEY, Frank. 1915. *A History of the Japanese People from The Earliest Times to The End of The Meiji Era*, New York: The Encyclopaedia Britannica Co.

CARTWRIGHT, Mark. 28 June 2019. *Sengoku Period*, World History Encyclopedia, article can be read at: https://www.worldhistory.org/Sengoku_Period/

CORTAZZI, Hugh. 1990. *The Japanese Achievement*, London: Sidgwick and Jackson.

CULEDDU Paola, Maria. 2008. *Daimyo Principles in the Tokugawa Era: An essay on Itakura Shigenori and some of his contemporaries*, Rivista Studi Orientali.

CULEDDU, Paola, Maria. 2018. *The Evolution of the Ancient Way of the Warrior: From the Ancient Chronicles to the Tokugawa Period*, Asian Studies VI (XXII).

HALL, Whitney, John. 1991. *The Cambridge History of Japan: Volume 4 Early Modern Japan*, Cambridge University Press.

HENSHALL, Kenneth. 2012. A *History of Japan: From Stone Age to Superpower*, Palgrave Macmillan, third edition.

LATZ, Gil, NOTEHELFER, Fred G., SAKAMOTO, Taro, JANSEN, Marius B., Watanabe, Akira, Masamoto, Kitajima, Toyoda, Takeshi, Masai, Yasuo, Hurst, G. Cameron and Hijino, Shigeki. 30 Sep. 2021, *Japan*, *Encyclopedia Britannica*, article can be read at: https://www.britannica.com/place/Japan

MASON, R.H.P., Caiger J.G. 1997. *A History of Japan*, Tuttle Publishing.

OLIVER, Christine. 1992. *The antecedents of deinstitutionalization*. Organization Studies. 13(4) 563 – 588.

SHELTON Woods. *The Three Unifiers of Sengoku Era Japan*, Japan Society, article can be read at: https://aboutjapan.japansociety.org/the-three-unifiers-of-sengoku-era-japan

STEBEN, Barry D. 2002. *Rai San'yo's Philosophy of History and the Ideal of Imperial Restoration*, in: East Asian History, number 24, Institute of Advanced Studies Australian National University.

TURNBULL, Stephen. 1996. *Samurai Warfare*, USA: Sterling Publishing Co.

TURNBULL, Stephen. 2002. *War in Japan 1467-1615*, Osprey Publishing Limited.

TZU, Sun, 2000, *The Art of War*, England: Allandale Online Publishing.

INDEX OF AUTHORS

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Director: Laura MÎNDRICAN

The publications consists of 292 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

5/27.01.2022 C. 225/2021