“CAROL I” NATIONAL DEFENCE UNIVERSITY
CENTRE FOR DEFENCE AND SECURITY STRATEGIC STUDIES

STRATEGIC IMPACT

No. 2 [87]/2023

Open-access academic quarterly, nationally acknowledged
by CNATDCU, indexed in CEEOL, EBSCO, Index Copernicus,
ProQuest, WorldCat and ROAD international databases

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

CONTACT ADDRESS

Șos. Panduri, no. 68-72, Sector 5, 050662, Bucharest, Romania
Phone: +4021.319.56.49; Fax: +4021.319.57.80
Website: https://cssas.unap.ro/index_en.htm
E-mail: impactstrategic@unap.ro

ISSN 1841-5784; ISSN-L 1841-5784; e-ISSN 1842-9904

CONTENTS

EDITOR'S NOTE

The 87th edition of *Strategic Impact* journal, the second in 2023, comprises five articles which deal with subjects of interest in the field of security studies, followed by the ***Strategic Dialogue*** rubric and the ***Guide for authors***.

The first rubric, ***Political-Military Topicality***, brings to your attention an article written in co-authorship by our colleagues, Senior Researcher Alexandra Sarcinschi, PhD, and Senior Researcher Cristian Băhnăreanu, PhD. It explores a trend referring to a continuation of the international struggle for power as traditional Realism defines it, but with sources of power to be explored according to the current trends in the security environment, medical resources and a continuing development of military power, respectively.

In the ***NATO and EU: Policies, Strategies, Actions*** rubric we have included an article written by Mr. Dragoș Ilinca, which is aiming to bring into light the way in which Common Security and Defence Policy (CSPD) answers to the challenge of consolidating resilience, and, in the context of the war in Ukraine, a special note is made on how the latest EU strategic document (Strategic Compass) considered resilience as being one of the strategic objectives of CSDP.

The rubric ***Security and Military Strategy*** includes an article co-authored by Mr. Endre Szűcs PhD and Mr. Miklós Szakali, PhD Candidate. The article examines the possibility to ensure complex military and civilian capabilities corresponding to complex security challenges, while also considering the development and the usability of the defence planning system, generated and used by the military to provide civilian capabilities.

The rubric ***Information Society*** presents key elements regarding the use of virtual assets in illicit activities by sanctioned entities. The author, Mr. Bogdan Vacusta highlights the necessity to increase defence and intelligence resources for better data analysis on this type of entities.

The fifth rubric, ***Intelligence Studies***, comprises an article written by Mr. Attila Mate Kovacs, which deals with the topic of ransomware attacks on the healthcare industry. The focus is on how the detection and prevention of the attacks could be counteracted by constantly improving the skills of cybersecurity experts, by collecting and analysing large volumes of data and applying soft computing techniques.

In this edition, we publish a ***Strategic Dialogue*** with the President of the Romanian Reserve Officers Association, Lieutenant General (r.) Virgil Bălăceanu, PhD, in the endeavour to clarify some of the most interesting topical subjects: challenges and realities of the Romanian Armed Forces' Reserve; the feasibility in implementation of the Voluntary Military Service; main issues of Romanian Defence Industry, and the War in Ukraine.

Also, this edition includes the ***Guide for authors***, a mandatory reading for those who wish to disseminate the research results in our journal.

For those discovering *Strategic Impact* for the first time, the publication is an open-access peer reviewed journal, edited by the Centre for Defence and Security Strategic Studies and published with the support of "Carol I" National Defence University Publishing House, and, also, a prestigious scientific journal in the field of military sciences, information and public order, according to the National Council for Titles, Diplomas and Certificates (CNATDCU).

Strategic Impact is an academic publication in the field of strategic defence and security studies journal that has been published since 2005 in English, in print and online. The articles are checked for plagiarism and scientifically evaluated (double blind peer review method). The thematic areas include political science, international relations, geopolitics, the political-military sphere, international organizations – with a focus on NATO and the EU information society, cyber security, intelligence studies and military history. Readers will find in the pages of the publication strategic-level analyses, syntheses and evaluations, views that explore the impact of national, regional and global dynamics.

In terms of international visibility − the primary objective of the publication − the recognition of the scientific quality of the journal is confirmed by its indexing in the international databases CEEOL (Central and Eastern European Online Library, Germany), EBSCO (USA), Index Copernicus (Poland), ProQuest (USA), and WorldCat and ROAD ISSN, as well as its presence in the virtual catalogues of the libraries of prestigious institutions abroad, such as NATO and military universities in Bulgaria, Poland, Czech Republic, Hungary, Estonia etc.

The journal is distributed free of charge in main institutions in the field of security and defence, in the academia and abroad − in Europe, Asia and America.

In the end, we encourage those interested in publishing in our journal to rigorously survey and assess the dynamics of the security environment and, at the same time, we invite students, master students and doctoral candidates to submit articles for publication in the monthly supplement of the journal, *Strategic Colloquium*, available on the Internet at http://cssas.unap.ro/ro/cs.htm, indexed in the international database CEEOL, Google scholar and ROAD ISSN.

Editor-in-Chief, Colonel Florian CÎRCIUMARU, PhD
Director of the Centre for Defence and Security Strategic Studies

DOI: 10.53477/1842-9904-23-08

A REALIST PERSPECTIVE ON THE WORLD BEFORE THE WAR IN UKRAINE: WAS THE PANDEMIC AN INHIBITOR OF THE STRUGGLE FOR POWER?

Alexandra SARCINSCHI, PhD*
Cristian BĂHNĂREANU, PhD**

The outbreak of the COVID-19 pandemic has prompted the world to consider an increase in international cooperation to manage this security threat, particularly under the WHO and with the support of the great powers. The surprise was that the WHO was accused of failure and the great powers developed protectionist and nationalist tendencies, with states coming to the fore once again as the most important actors in world politics. In this context, the paper explores a trend that continued to exist even during the pandemic, even though the war in Ukraine was clearly not on the international agenda: namely a continuation of the struggle for power as traditional Realism define it, but with new sources of power to be explored according to the current trends in the security environment: medical resources and a continuing development of military power, despite the economic problems that have arisen.

Keywords: *Realism; COVID-19 pandemic; state actors; struggle for power; public opinion; medical resources; military and economic power.*

**** Alexandra SARCINSCHI, PhD, is Senior Researcher within the Center for Defence and Security Strategic Studies, "Carol I" National Defence University, Bucharest, Romania. Email: sarcinschi.alexandra@unap.ro***
***** Cristian BĂHNĂREANU, PhD is Senior Researcher within the Center for Defence and Security Strategic Studies, "Carol I" National Defence University, Bucharest, Romania. Email: bahnareanu.cristian@unap.ro***

Introduction

Today's world is not what people expected three years ago. The COVID-19 pandemic has affected the entire mankind and has raised new concerns about issues not obviously related to security, such as medical resources and vaccination. They have been important so far, but more on the national healthcare agenda. Still, since the pandemic, these issues have become obvious vital resources for human survival and for the state itself. The paper briefly introduces a Realist approach on these resources as they have been used for the last two years not exclusively for humanitarian assistance, but also for accentuating the struggle for power (respectively, the first section). The analysis will be stopped before the moment of Russia's military aggression against Ukraine (February, 2022) because, since then, the pandemic has become a secondary issue and the military matters have once again become the hottest issues on the international agenda.

The question that arises here is whether moving the focus to the management of the COVID-19 pandemic and medical resources meant a declining interest in consolidating military and economic power. Or, in other words *have the great powers been slowed down by the COVID-19 pandemic in their struggle for power?*

Answering this question requires clarification of three main aspects: first of all, why the Realist perspective was chosen; secondly, what role did medical resources play in defining the struggle for power during this period of time, and thirdly, whether during the pandemic the struggle for power was hindered.

The choice for the Realist perspective is justified by the fact that the contemporary security environment shows that state actors have the most important role in managing a crisis of such magnitude and severity as the COVID-19 pandemic. In other words, as Stephen M. Walt wrote in 2020, "the present emergency reminds us that states are still the main actors in global politics" (Walt 2020), despite globalization. One of the arguments used is that, confronted with a new and dramatic threat, people turn to their governments as providers of safety and security (as an implication of states' nature as selfish actors that seek their own security – Realism), not to international organizations (Liberalism) or other people and ideas (Constructivism). Nevertheless, Realism does not exclude the role of non-state actors, but underlines their secondary importance and the fact that such actors are created by states in order to serve their own interests (Vasquez 2004) (Carlsnaes, Risse and Simmons 2013). In this pandemic context, states were the first actors to take action in taming the threat, despite UN (especially its agency, World Health Organization) and EU actions in managing the crisis.

The other two aspects will be clarified in the paper considering the classical Realist analysis on world politics focused on the great powers as defined before the war in Ukraine. This status is a consequence of the number of resources they possess, the way in which these resources are converted in capabilities, and how they are

applied as foreign policy instruments. Apart from the fact that the pandemic has brought to attention the issue of medical resources that were used by certain states in the struggle for power, as shown below, the resources emphasized by realists are natural/geographic, population, military and economic ones. That is why a brief analysis on specific indicators (the second section of the study) is required in order to validate the thesis that the COVID-19 pandemic did not end or at least slow down the efforts to maintain and increase the military and economic power of the great world actors (the United States, the Russian Federation, China, the United Kingdom, France, and especially as a result of the present trends in the security environment, Germany[1] and India).

The paper will show that state's efforts for managing the COVID-19 pandemic and the new focus on medical resources as sources of power have not prevented the struggle for military and economic power in Realistic terms.

1. The Revival of States as Main Actors in World Politics during the Pandemic

Realism is not a school of thought exempt from criticism. Otherwise, the progress in political science would be inexistent. Liberal, Constructivist, and Critical perspectives are the most important alternatives to Realism, each of them offering its own explanations on world politics (Nau 2019, 26-28).

The main assumption for a Realist approach of contemporary political world is that the state's role on international arena is growing as a result of the COVID-19 pandemic. This revival is correlated with individuals' loss of confidence in the main international organizations and growth of public trust in national government during the pandemic.

Why this correlation within a Realist framework and not Liberalism which argues that public support legitimizes the government or Constructivism which is more oriented towards ideas and people? From a sociological point of view, increased trust in national governments is the result of their approach to managing the pandemic and the failure of international organizations to respond to the crisis (or at least represented as such by population). In fact, bringing into question the issue of public opinion is not a digression from the Realist perspective. As H. J. Morgenthau states, anywhere in the world, public opinion on international issues is shaped by national policy institutions, not the other way around (Morgenthau 1997, 279). Moreover, the support of population is important for the success of one government's domestic and foreign policy. The balance between the foreign policy and the power to achieve it must be completed with the balance between various elements of national power. Population is one of those elements and popular support is one of the key requirements, apart from its number or government's capacity to protect it (Morgenthau 1997, 163-168).

It should be pointed out that public opinion is far from legitimizing the role of states as main actors in world politics, however it is an indicator of their revival in

[1] Even though Germany is not a nuclear power.

comparison with international organizations in the context of a crisis such as the COVID-19 pandemic. In this context, during the pandemic, the role of the state as *protector of population* was brought to the fore, and the issues of health, medical resources and the lockdown held leading positions on the public agenda.

As seen in Figure no. 1, between November 2019 (fieldwork for *Standard Eurobarometer 92*) and July 2020 (fieldwork for *Standard Eurobarometer 93*), trust in national government, regional or local public authorities and public administration increased with 6 pp, respectively 4 and 3 pp, while trust in UN decreased with 3 pp and recorded no changes for EU, although it remains below 50% for the last 6 years. The next three Eurobarometer shows a decrease of confidence in the government and public authorities (Winter 2020-2021), immediately followed by a return in trust in national authorities and an even sharper decline in the UN and EU (Spring 2021 and Winter 2021-2022).

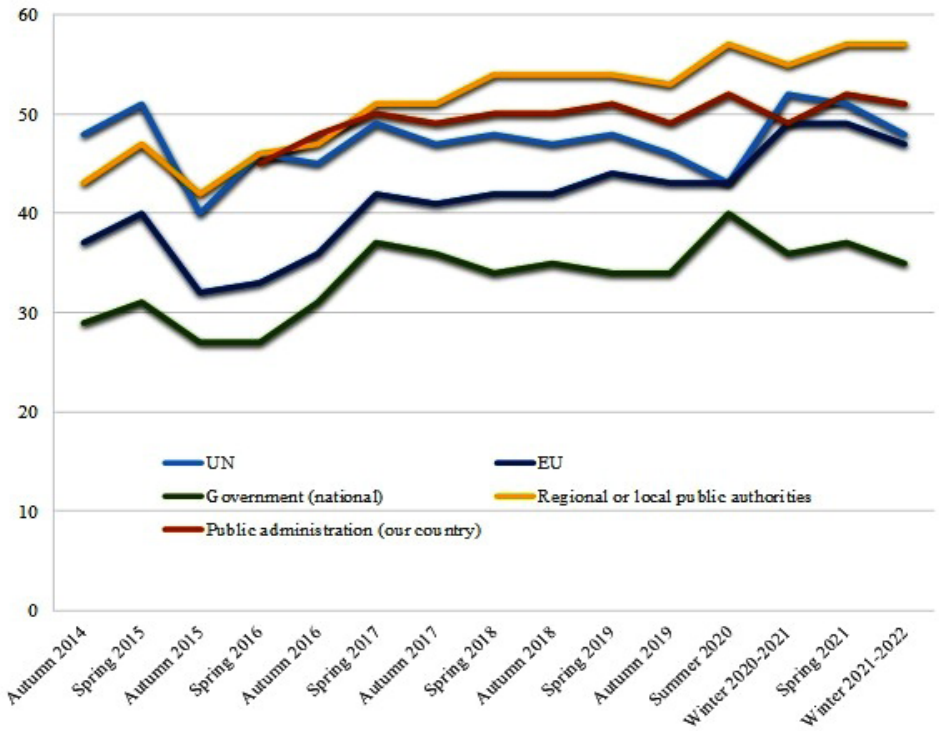

Figure no. 1: The answer to the question "How much trust you have in certain media and institutions?", according to *Standard Eurobarometer* 92 - 96 (% - tend to trust at EU level)[2]

[2] Data extracted from Standard Eurobarometer 92 - Autumn 2019 (EC November 2019), Standard Eurobarometer 93 - Summer 2020 (EC July-August 2020), Standard Eurobarometer 94 - Winter 2020-2021 (EC February-March 2021), Standard Eurobarometer 95 - Spring 2021 (EC June-July 2021), Standard Eurobarometer 96 - Winter 2021-2022 (EC January-February 2022) and Standard Eurobarometer 82-91 (EC 2014-2019).

This trend might be explained by the correlation between the economic effects of the pandemic and the pandemic fatigue, on the one hand, and the image of the government as the main actor in managing this crisis. Also, it could be categorized as a perverse effect of the crisis management efforts (Figures no. 2-3) and does not imply the fact that state is no longer the main actor in its management. According to Realists, it shows that public opinion approves or disapproves of government actions, but is not stable and is influenced by various factors.

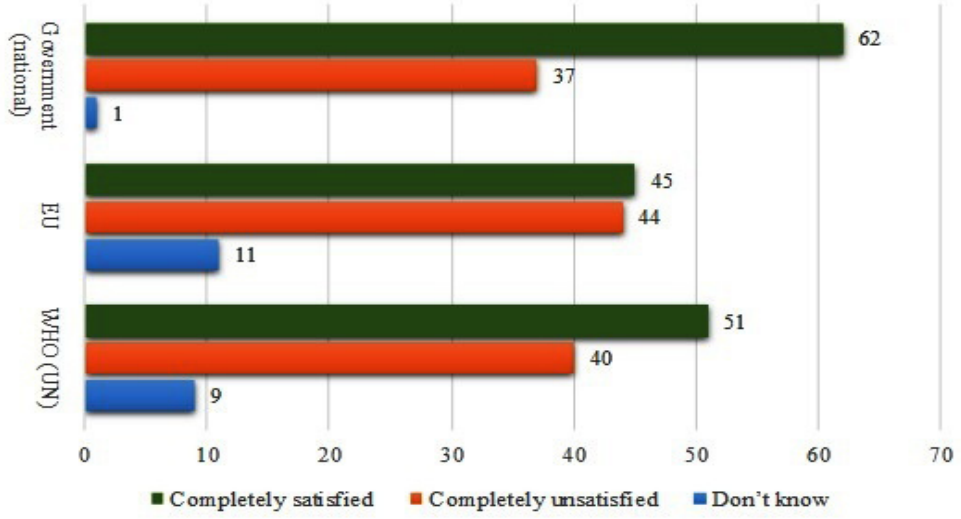

Figure no. 2: The answer to the question "In general, how satisfied are you with the measures taken to fight the Coronavirus outbreak by…?", according to *Standard Eurobarometer* 93 (% - tend to trust at EU level)[3]

Table no. 1: The answer to the question "In general, how satisfied are you with the measures taken to fight the Coronavirus outbreak by…?", according to *Standard Eurobarometer* 94 - 96 (% - tend to trust at EU level)[4]

	Completely satisfied			Completely unsatisfied			Don't know		
	EB 94	*EB 95*	*EB 96*	*EB 94*	*EB 95*	*EB 96*	*EB 94*	*EB 95*	*EB 96*
Government (national)	43	46	48	56	53	50	1	1	2
EU	43	41	42	49	51	49	8	8	9

[3] Data extracted from Standard Eurobarometer 93 - Summer 2020 (EC July-August 2020).
[4] Data extracted from Standard Eurobarometer 94 - Winter 2020-2021 (EC February-March 2021), Standard Eurobarometer 95 - Spring 2021 (EC June-July 2021), Standard Eurobarometer 96 - Winter 2021-2022 (EC January-February 2022).

In addition, there is a marked gap between population's satisfaction with measures taken by various state and non-state actors in fighting the pandemic (Figures no. 2 and Table no. 1).

In the summer of 2020, if the difference between satisfaction and dissatisfaction of population with measures taken by national government is 25 pp, it is lower in the case of EU and WHO (UN) (Figure no. 2). The perverse effect mentioned above is to be seen also in measuring satisfaction with the measures taken to fight the Coronavirus outbreak (Table no. 1). The last three Standard Eurobarometer before the war shows a decrease in satisfaction both in the case of national governments and the EU, but it does not address the issue of WHO (UN).

In this context, one might argue that the societal trends contradict these opinion polls: the 2020-2021 period showed an increase in the number of social protests against restrictions imposed by national governments from EU countries. An exhaustive analysis reveals that, on the one hand, these protests were rather the result of *pandemic fatigue* and economic problems caused by the *lockdown* and other restrictive measures, and, on the other hand, there are signs that some of them were organized by far-right movements (Sarcinschi 2020). Actually, the Standard EB93 shows that more than 80% of the European respondents think that the limitation of civil liberties was justified in fighting the pandemic (Figure no. 3).

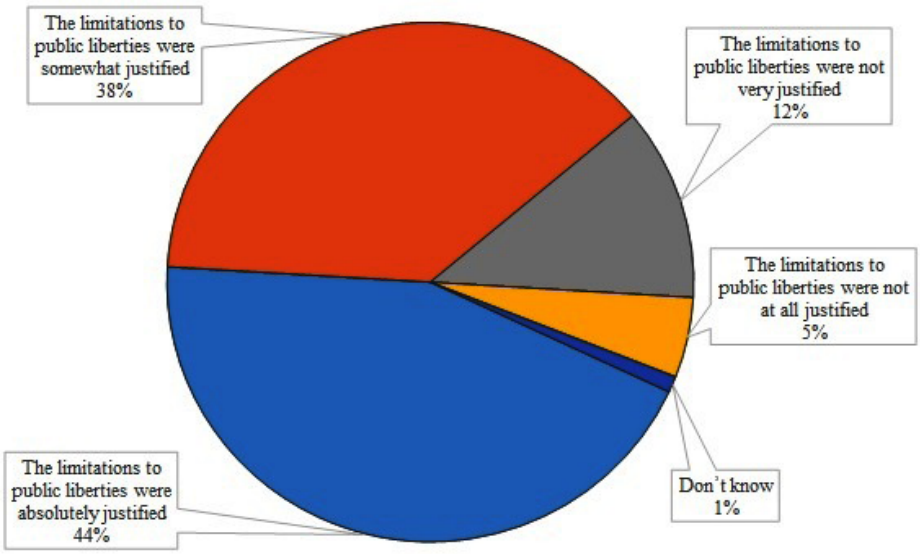

Figure no. 3: The answer to the question "Thinking about the measures taken by the public authorities in (our country) to fight the Coronavirus and its effects, would you say that...", according to *Standard Eurobarometer 93* (% - EU)[5]

[5] Data extracted from Standard Eurobarometer 93 - Summer 2020 (EC July-August 2020).

In the last Standard EB (Table no. 2), the answers to the question regarding the support for the measures taken by public authorities excluded the term "limitation to public liberties" and focused on "restriction measures". Even if the overall support to such measures fell below 75%, the degree of acceptance is still high and the trend preserves.

Table no. 2: The answer to the question "Thinking about the restriction measures taken by the public authorities (in our country) to fight the Coronavirus and its effects, would you say that they were...", according to *Standard Eurobarometer 94 - 96* (% - EU)[6]

	Absolutely justified	Somewhat justified	Not very justified	Not at all justified	Don't know
B 94	27	46	19	7	1
B 95	27	47	19	6	1
B 96	22	47	21	9	1

The main assumption – the COVID-19 pandemic has reconfirmed states as the most important actors in global politics − is to be validated also by bringing into debate issues such as *vaccine race*, *mask diplomacy*, and *vaccine nationalism* (Blog by HR/VP Josep Borrell 2020) (Ramscar 2020). These trends can be correlated with the Realist perspective on the pandemic. Firstly, the nation that will win the *vaccine race*[7] – defined as a competition for a vaccine with the highest success rate, not only to tame the pandemic, but also to enhance national pride and international image[8] – will gain *greater prestige* in global politics taking into account that prestige politics is a component of the struggle for power (Morgenthau 1997, 52-57). Secondly, *mask diplomacy*[9] might be a form of achieving *political compliance or obedience* by exploiting the need for scarce medical resources (placing the medical resources in the same category of *hard power* sources as military and economic ones[10]).

[6] Data extracted from Standard Eurobarometer 94 - Winter 2020-2021 (EC February-March 2021), Standard Eurobarometer 95 - Spring 2021 (EC June-July 2021), Standard Eurobarometer 96 - Winter 2021-2022 (EC January-February 2022).

[7] In this case, Germany was the winner with the Pfizer vaccine developed by BioNTech, in late 2020.

[8] See the name given to the vaccines or their development programs: Operation *Warp Speed* (the US), *Sputnik V* (the Russian Federation), *Sinovac* (China), the *BlessedCOVIran* (Iran), etc.

[9] For example, China donated masks and medical supplies in order to rehabilitate its negative international image as source of the SARS-CoV-2 virus (Hornung 2020). Instead, the US prohibited the export of five types of personal protective equipment without explicit approval, but offered its support for friends and partners, excepting China (The White House 2020a), and Trump administration threatened to withdraw from the WHO and suspend financing if it did not take action against the Asian state (The White House 2020b). The US withdrawal process was halted by the Biden administration (The White House 2021).

[10] This assumption is detailed in a 2020 paper (Sarcinschi November 2020).

Not last, *vaccine nationalism* – a situation in which a country strives to gain first access to vaccine supply and accumulate key-components for vaccine production (Hafner, et al. 2000) (Guterres 2021) – shows that states are selfish actors seeking their own security.

Therefore, the COVID-19 pandemic gave states the opportunity to reaffirm their role as a major player in international politics in a Realist manner. If the general image is that they are cooperating in order to manage the pandemic (see cooperation initiatives whose success have partly materialized, such as Gavi, the Vaccine Alliance and EU initiatives), their actions show even a cynical zero-sum game, in which one state's gain means an equal loss by another.

2. The Impact of the COVID-19 Pandemic on Main Sources of Power

As Realists argue, power derives from a state actor's possession of resources in relation to other actors. In this context, an analysis of world powers must be focused on the comparison between the most important sources of power, especially the material ones of a military and economic nature. Even though this section focuses on military power, this does not mean that the evaluation of one nation's overall power must be performed by only one factor to the detriment of others. As H. J. Morgenthau argues, the process of power evaluation must take into account the fact that power is relative, it is not permanent and that evaluation must not be carried out by a single factor (Morgenthau 1997, 170-183). Still, for most classical Realists, all great powers allocate considerable resources to develop their military capabilities for future crisis and conflicts.

The following analysis is focused on the five Permanent Members of the UN Security Council (China, France, Russian Federation, the United Kingdom, and the United States) and Germany, as the EU's economic engine, also India, who is seeking the status of major power.

The issue that arises in this context is whether or not the Realist competition for power has been hindered by the COVID-19 pandemic. Theoretically, this crisis has affected the process of maintaining and increasing military power on many dimensions: both the quantity and quality of active military personnel and reserve (the infection with SARS-CoV-2 of a large number of soldiers, the cancellation of training and military exercises, many activities were conducted online), the defence budgets (adjustments as a result of the economic crisis), the military procurement programs and the operationalization of force structures (cuts in military spending), the interoperability (reducing joint planning, training and exercises), etc. In order to verify these assumptions, we will follow the evolution of military budgets in recent years, the acquisition of military technology and techniques, including in the nuclear and space spheres.

Since economic resources are one of the foundations of military power, the analysis of statistical data shows the evolution of GDP in all analysed countries between 2017-2019, and during the COVID-19 pandemic' (2020-2021) (Figure no. 4).

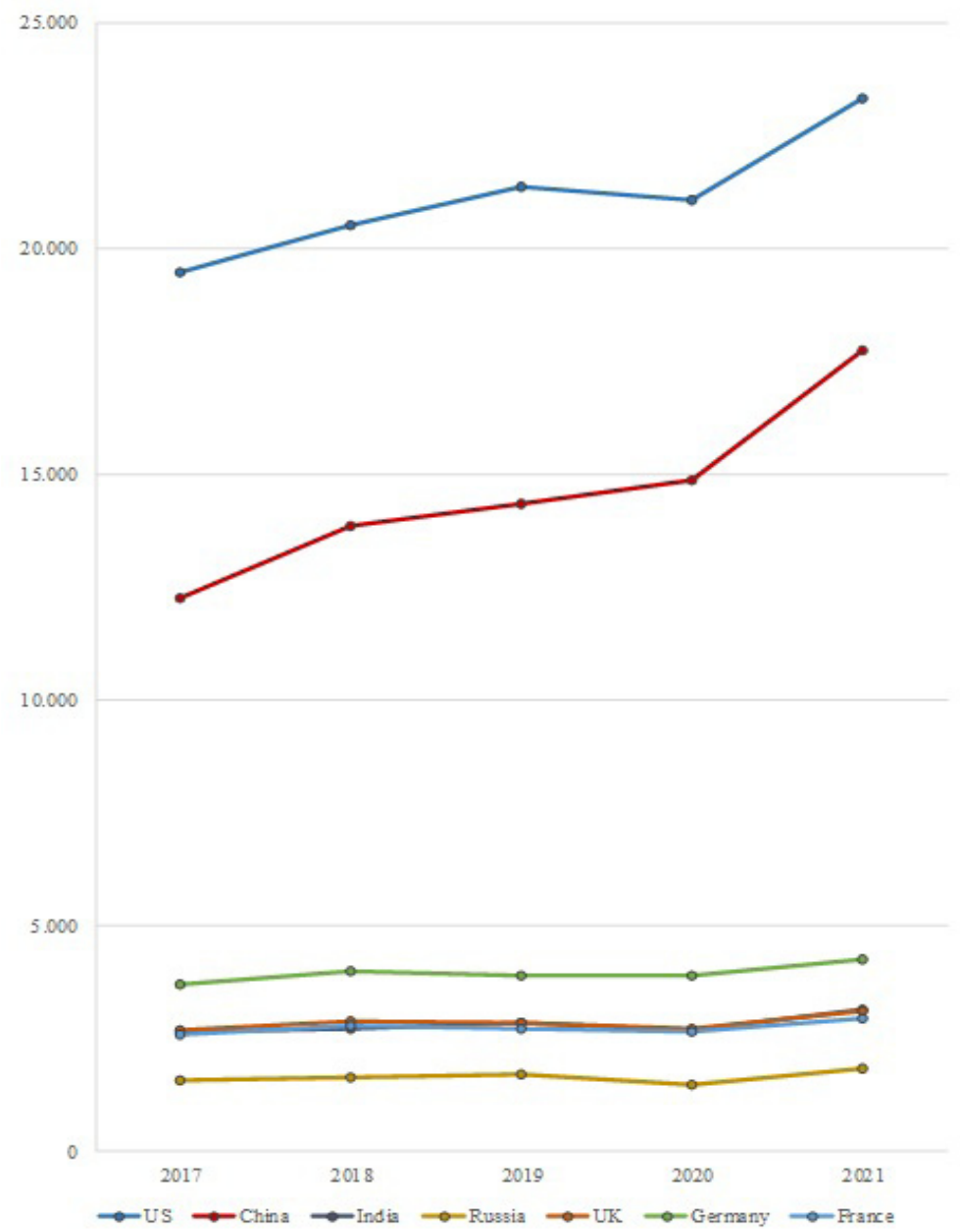

Figure no. 4: Great powers' GDP evolution in the period 2017-2021, according to *IMF Database* (billions USD)[11]

[11] Data extracted from *World Economic Outlook Database (April 2023 Edition)* (IMF April 2023).

The measures taken by national authorities in the second quarter of 2020 to prevent the spread of the coronavirus led to significant declines in almost all economic sectors (especially tourism, hospitality, air transport, automotive industry, and retail), crash of the stock markets, job losses, negative oil prices, disruption of world trade, etc. Amid stimulus packages and the imminent arrival of vaccines, there was hope for an economic recovery in the second half, but the next wave of the pandemic ruined those plans and global economy recorded GDP decline by 3.4% in 2020 (UN 2022, 4). Although all countries under analysis, excepting China, experienced an economic contraction in 2020, the data for 2021 shows growth in all cases as a result of the population vaccination campaigns and economic support programs. This picture did not translate into the area of military budgets, as defence spending continued to increase in 2020-2021, with only Russia and the US seeing a small decrease at the end of 2020 and 2021, respectively (Figure no. 5).

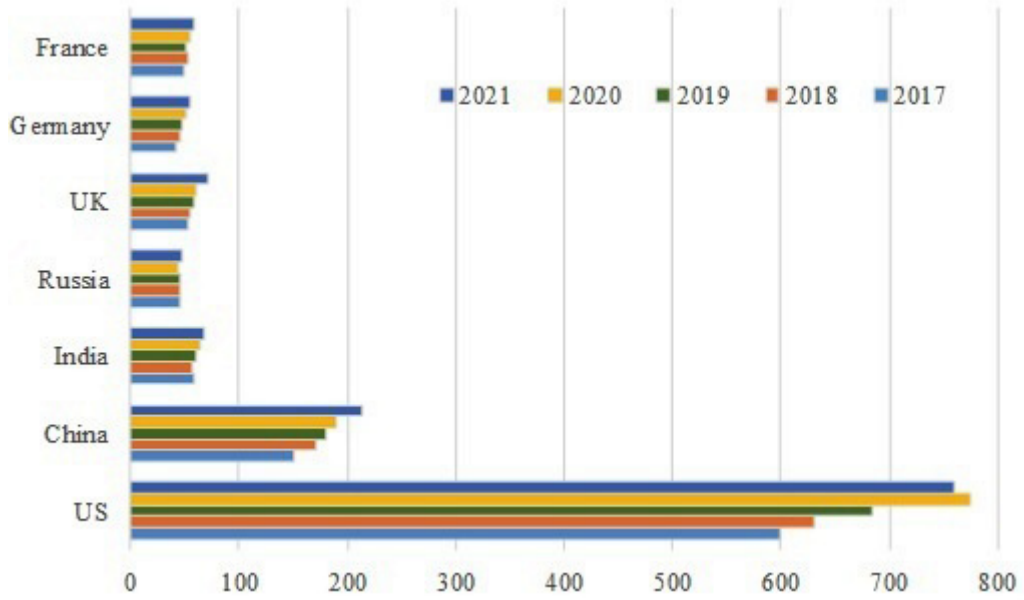

Figure no. 5: Great powers' military budget evolution in the period 2017-2021, according to The Military Balance (billions USD)[12]

Although the COVID-19 pandemic has affected world's economy, most of the great powers have continued to increase the number of military technologies, weapons and equipment. For instance, the champions of acquisition, before the war in Ukraine, were China, Russia and India, each of them increasing in 2021 compared to 2020 the number of main battle tanks (+87 – Russia and +50 – India), infantry fighting vehicles (+640 – China and +120 – Russia), artillery (+881 – Russia,

[12] Data extracted from *The Military Balance (2019-2023 editions)* (IISS February 2019-2023)

+630 – China, +50 – India), armoured personnel carriers (+400 – China), attack helicopters (+30 – China, +5 – Russia), intercontinental ballistic missiles (+12 – China. +3 – Russia), tactical submarines (+34 – Russia), cruisers/destroyers/corvettes/frigates (+23 – China, +3 – Russia) (IISS February 2019-2023). Also, even as the global stockpile of nuclear warheads fell to 12,705 units in early 2022, the world's nuclear powers continued to upgrade their arsenals (SIPRI September 2022, 342). During the pandemic up to the reference time chosen in the analysis, Russia continued a significant modernization process of its nuclear forces, including testing the RS-28 Sarmat intercontinental ballistic missile (CSIS 2021). Moreover, China and India increased the number of warheads to 350 and 160 in January 2022 (SIPRI September 2022, 342) from 320 and 150 in 2020 (SIPRI September 2020, 326) and even 290 and 130-140 in 2019 (SIPRI September 2019, 288). Another example is the United Kingdom which, due to the increased volatility of the security environment, was planning in 2021 to increase the nuclear warhead stockpile to 260 even if the initial target (in 2010) was to reduce it from 225 to no more than 180 in the mid-2020s (HM Government March 2021, 76). Over the period 2017-2021, the US has reduced its number of nuclear warheads by more than 1,000, from 6,450 (SIPRI November 2018, 238) to 5,428 (SIPRI September 2022, 344), but plans to spend 1.5 trillion dollars in the next 30 years on maintenance and upgrading its arsenal (CACNP 2021).

Another important aspect in developing national power is the space dimension (Table no. 3).

Table no. 3: The number of orbital launches in 2020 and 2021 and the number of military satellites operated by great powers at the end of 2021[13]

Number of	US	China	India	Russia	UK	Germany	France
Orbital launches in 2020	44	39	2	17	5 (EU)		
Orbital launches in 2021	51	56	2	25	6 (EU)		
Military satellites in 2021	233	139	9	101	6	7	18

Michael Sheehan argues that even if space has proven to be a domain where non-military aspects of power can be exploited in an advantageous manner, the result might still be a struggle for power and influence in the global system (Sheehan 2007, 13-15). As shown above, during 2020-2021, the pandemic has not impeded the development of various space programs, the great powers showing a special interest in this domain, of which the US, China and Russia exploit an impressive number of satellites for military use.

[13] Data extracted from *UCS Satellite Database* - updated on 01.01.2022 (Union of Concerned Scientists 2022) and *Wikipedia, the free encyclopedia* - since the official statistics on overall number of orbital launches is scarce and disparate, the source for above data are the following entries: "2021 in spaceflight" (Wikipedia 2022) and "2020 in spaceflight" (Wikipedia 2021).

However, why is the study of public opinion, as presented in the first section of the paper, relevant for a Realist analysis of sources of power, since this theory argues that the states' foreign agenda is not influenced by public opinion? The first section has shown that public opinion, even if does not legitimize states as main actors in world politics, is an indicator of its revival in comparison with international organizations. If one would think that the pandemic situation will impede states in strengthening their power and acting in the logic of power politics, the analysis of public opinion shows that even the main subjects of interest for the population (Figure no. 6) are far from the issue of military power, states dedicate great resources to improving it, as shown in this section. Europeans believe that the most important issues their countries are facing with today are health problems (35% on average in surveys analysed), rising prices/inflation/cost of living (27% on average), the economic situation (26% on average), and unemployment (20% on average), while great powers (including European powers) focus on improving their military capabilities despite the social situation and economic problems related to the COVID-19 crisis.

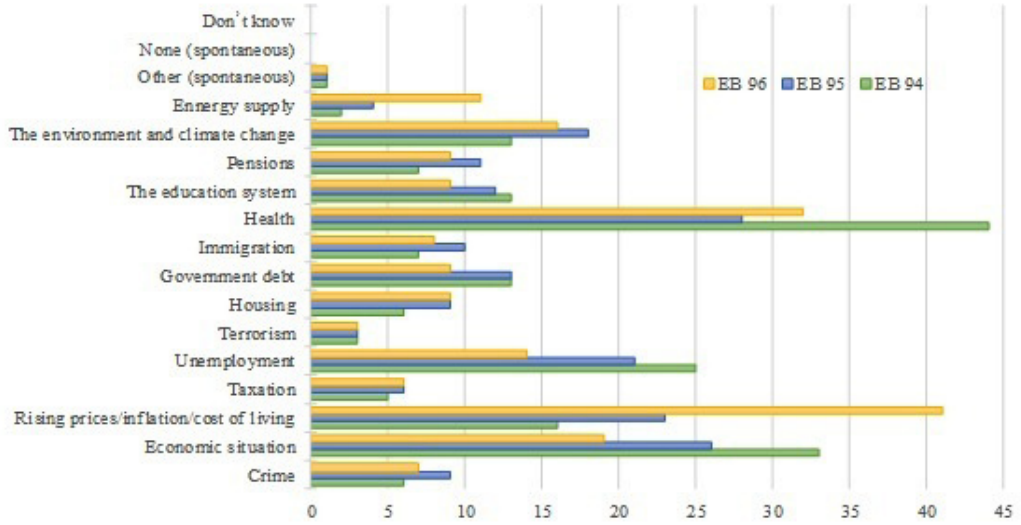

Figure no. 6: The answer to the question "What do you think are the two most important issues facing (our country) at the moment?", according to *Standard Eurobarometer 94-96* (% - EU)[14]

As shown above, data synthetized in this chapter represents only parts of a larger picture regarding nations' military power. Still, they are enough to understand that, from a Realist perspective, the ultimate benchmark of national power is military capability (Tellis, et al. 2000).

[14] Data extracted from Standard Eurobarometer 94 - Winter 2020-2021 (EC February-March 2021), Standard Eurobarometer 95 - Spring 2021 (EC June-July 2021), Standard Eurobarometer 96 - Winter 2021-2022 (EC January-February 2022).

Conclusions

The purpose of this paper is not to offer a geopolitical essay on today's world, but rather a brief analysis of the main Realist landmarks translated into a globalized world that has faced a new threat. Therefore, the COVID-19 pandemic has brought into attention the issue of states as relevant actors of world politics, to the detriment of international organizations whose role in managing the crisis was criticized by both individuals and governments. However, the revival of state in world politics is accompanied by various pitfalls that validate the translation of specific Realist concepts in a contemporary analysis of International Relations. The struggle for power is one of those concepts and it is illustrated by trends such as *vaccine race*, *mask diplomacy*, and *vaccine nationalism*. They correspond to one of the fundamental patterns of politics, *prestige politics*, that concerns maintaining or increasing the power of a nation. All three of them have been used mainly by the US, China, and Russia to demonstrate their power, by means of medical resources, although the entire world has been suffering from the pandemic.

An important observation correlated with the world's current state is that *medical resources*, most valued in pandemic times, are just beginning to be part of world politics whether referring to *hard power*, *soft power* or *smart power*. A further step in this direction is to explore the validity of the assertion that medical resources are sources of power, more precisely hard power. This is a crucial perspective since the implementation of Realist power politics into the area of global health might impede non-state actors' capacity to predict, identify and manage threats to health security.

Moreover, neither the economic crisis triggered by the pandemic nor the competition for medical resources and vaccines has stopped the development of military power. The most important states of the world show a desire to continue the competition for power in a classical Realist manner. It is important to underline that since the military capabilities are used both for defending and for enabling states to pursue their interests, the continued competition for power, extended even in the area of medical resources, proves that Realist principles are still valid and world's complexity is generated by power stratification and competing self-interests of states. The war in Ukraine demonstrates that the most powerful countries have continued to build up their military power to prepare for future crisis and conflicts: in this case, Russia for invasion, Ukraine and NATO member states for defence.

BIBLIOGRAPHY:

Blog by HR/VP Josep Borrell. 2020. *No to vaccine nationalism, yes to vaccine multilateralism*. The Diplomatic Service of the Europen Union, 13 November. Accessed March 6, 2023. https://www.eeas.europa.eu/eeas/no-vaccine-nationalism-yes-vaccine-multilateralism_en.

CACNP. 2021. *Fact Sheet: U.S. Nuclear Weapons Modernization: Costs & Constraints.* Washington, D.C.: Center for Arms Control and Non-Proliferation, 22 January. Accessed March 23, 2023. https://armscontrolcenter.org/fact-sheet-u-s-nuclear-weapons-modernization-costs-constraints.

Carlsnaes, Walter, Thomas Risse, and Beth A. Simmons. 2013. *Handbook of International Relations.* Second Edition. London: SAGE Publications Ltd.

CSIS. 2021. "Missiles of Russia." *The CSIS Missile Defense Project.* Washington, D.C.: Center for Strategic and International Studies, 10 August. Accessed March 21, 2023. https://missilethreat.csis.org/country/russia.

EC. 2014-2019. "Standard Eurobarometer." Survey, European Commission, Bruxelles. Accessed February 27, 2023. https://europa.eu/eurobarometer/surveys/browse/all/series/4961.

EC. November 2019. "Standard Eurobarometer 92 - Autumn 2019 - Annex." Survey, Directorate-General for Communication, European Commission, Bruxelles. Accessed February 27, 2023. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=72800.

EC. July-August 2020. "Standard Eurobarometer 93 - Summer 2020 - Annex." Survey, Directorate-General for Communication, European Commission, Bruxelles. Accessed February 27, 2023. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=73627.

EC. February-March 2021. "Standard Eurobarometer 94 - Winter 2020-2021 - Annex." Survey, Directorate-General for Communication, European Commission, Bruxelles. Accessed February 27, 2023. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=76407.

EC. June-July 2021. "Standard Eurobarometer 95 - Spring 2021 - Annex." Survey, Directorate-General for Communication, European Commission, Bruxelles. Accessed February 27, 2023. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=76729.

EC. January-February 2022. "Standard Eurobarometer 96 - Winter 2021-2022 - Annex." Survey, Directorate-General for Communication, European Commission, Bruxelles. Accessed February 27, 2023. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=81059.

Guterres, António. 2021. "Vaccine Nationalism, Hoarding Putting Us All at Risk, Secretary-General Tells World Health Summit, Warning COVID-19 Will Not Be Last Global Pandemic." *Statements and messages.* Berlin, 24 October. Accessed March 6, 2023. https://press.un.org/en/2021/sgsm20986.doc.htm.

Hafner, Marco, Erez Yerushalmi, Clement Fays, Eliane Dufresne, and Christian Van Stolk. 2000. *COVID-19 and the cost of vaccine nationalism.* RAND. Accessed March 6, 2023. https://www.rand.org/pubs/research_reports/RRA769-1.html.

HM Government. March 2021. "Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy." Policy paper. Accessed March 23, 2023. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

Hornung, Jeffrey W. 2020. "Don't Be Fooled by China's Mask Diplomacy." *The RAND Blog*. 5 May. Accessed March 6, 2022. https://www.rand.org/blog/2020/05/dont-be-fooled-by-chinas-mask-diplomacy.html.

IISS. February 2019-2023. *The Military Balance, 2019-2023 editions.* The International Institute for Strategic Studies, London: Routledge.

IMF. April 2023. *World Economic Outlook Database*. Washington, D.C.: International Monetary Fund. Accessed May 8, 2023. https://www.imf.org/en/Publications/WEO/weo-database/2023/April.

Morgenthau, Hans J. 1997. *Politics among Nations. The Struggle for Power and Peace.* Sixth Edition. Beijing: Peking University Press.

Nau, Henry R. 2019. *Perspectives on International Relations. Power, Institutions, and Ideas.* Sixth Edition. Los Angeles: CQ Press.

Ramscar, Helen. 2020. "Vaccine Nationalism in the Age of Coronavirus." *RUSI Commentary.* 19 May. Accessed March 6, 2023. https://rusi.org/explore-our-research/publications/commentary/vaccine-nationalism-age-coronavirus.

Sarcinschi, Alexandra. November 2020. "Potential new sources of power in international politics. Case study: COVID-19 pandemic and health resources." *Proceedings of the International Scientific Conference Strategies XXI - The Complex and Dynamic Nature of the Security.* Bucharest: "Carol I" National Defence University Publishing House. 114-123.

Sarcinschi, Alexandra. 2020. "Race for Vaccine and Medical Resources: A New Side of the Struggle for Power on the International Arena." *Strategic Impact* ("Carol I" National Defence University Publishing House) (4(77)): 7-23.

Sheehan, Michael. 2007. *The International Politics of Space.* London: Routledge.

SIPRI. November 2018. *SIPRI Yearbook 2018: Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute, Oxford University Press.

SIPRI. September 2019. *SIPRI Yearbook 2019: Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute, Oxford University Press.

SIPRI. September 2020. *SIPRI Yearbook 2020: Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute, Oxford: Oxford University Press.

SIPRI. September 2022. *SIPRI Yearbook 2022: Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute, Oxford University Press.

Tellis, Ashley J., Janice Bially, Christopher Layne, and Melissa McPherson. 2000. *Measuring National Power in the Postindustrial Age.* Santa Monica: RAND Corporation. Accessed March 29, 2023. https://www.rand.org/pubs/monograph_reports/MR1110.html.

The White House. 2021. "Letter to His Excellency António Guterres." *Statements & Releases.* Washington, D.C., 20 January. Accessed March 6, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/20/letter-his-excellency-antonio-guterres.

The White House. 2020a. "Remarks by President Trump to the 75th Session of the United Nations General Assembly." *Remarks.* Washington, D.C., 22 September. Accessed March 6, 2023. https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-75th-session-united-nations-general-assembly.

The White House. 2020b. "The Letter of the US President, Mr. Donald Trump, to His Excellency, Dr. Tedros Adhanom Ghebreyesus, Director-General of the WHO." *Statements & Releases.* Washington, D.C., 18 May. Accessed March 6, 2023. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/05/Tedros-Letter.pdf.

UN. 2022. *World Economic Situation and Prospects 2022.* Department of Economic and Social Affairs, New York: United Nations.

Union of Concerned Scientists. 2022. *UCS Satellite Database.* Cambridge, 1 January. Accessed March 29, 2023. https://www.ucsusa.org/resources/satellite-database.

Vasquez, John A. 2004. *The Power of Power Politics. From Classical Realism to Neotraditionalism.* Cambridge University Press.

Walt, Stephen M. 2020. "The Realist's Guide to the Coronavirus Outbreak." *Foreign Policy.* Washington, D.C., 9 March. Accessed February 14, 2023. https://foreignpolicy.com/2020/03/09/coronavirus-economy-globalization-virus-icu-realism.

Wikipedia. 2021. *2020 in spaceflight.* Accessed March 29, 2023. https://en.wikipedia.org/wiki/2020_in_spaceflight.

Wikipedia. 2022. *2021 in spaceflight.* Accessed March 29, 2023. https://en.wikipedia.org/wiki/2021_in_spaceflight.

DOI: 10.53477/1842-9904-23-09

STRUCTURING RESILIENCE IN THE CONTEXT OF COMMON SECURITY AND DEFENCE POLICY

Dragoș ILINCA, PhD*

Resilience is a dimension with a pronounced multidisciplinary character covering a wide range of areas of society, which gives it a fluid profile and difficult to fit into a conceptual-functional typology. The interest in resilience is undoubtedly one of the trends of the current decade, however precursory elements are found throughout history in the most diverse forms of manifestation. As in the case of other dimensions explored in recent years from the perspective of European cooperation in the field of security and defence, resilience was quickly integrated into the steps carried out under the auspices of the Common Security and Defence Policy (CSDP), becoming one of the key objectives of the European Union's external action toolkit and, last but not least, of the operational commitments carried out globally by this organization. The contribution of the EU Global Security Strategy (EUGS) in designing resilience as a central element of the European security and defence cooperation agenda was defining. The main direction promoted by the EUGS was to strengthen resilience aspects in external action, while taking a structured approach to exploring options for strengthening internal resilience. Subsequently, the outbreak of the war in Ukraine as a result of Russia's aggression additionally valued the strategic significance of states' resilience and, subsequently, the importance of the EU's contribution in this direction.

This study is aiming to bring into light the way in which CSDP answers to the challenge of consolidating the resilience. In this vein, the methodological approach that was implemented responded the multidisciplinary character of this topic. In order to consolidate the comprehensive character of the present study, a historical perspective has been used that correlates the evolution of resilience in EU context with the development of various CSDP instruments. In this sense, an important

**** Dragoș ILINCA, PhD, is Research Coordinator within the Institute for Political Studies and Military History of Ministry of National Defence, Bucharest. Romania. E-mail: dilinca@yahoo.com***

direction of research is represented by the interaction between resilience and EU's external action and how the EU response to crisis situations has evolved. To a similar extent, this paper approached the resilience from the perspective of internal security of European Union, especially in the context of the war in Ukraine. A special note is made on how the latest EU strategic document (Strategic Compass) placed resilience as being one of the strategic objectives of CSDP. Given all of these aspects, the main conclusions of the article are emphasising the importance of adequate calibration of national approach in generating resilience, not only in the conceptual area but also on the practical aspects such as capabilities and resources required by a strong resilience. At the same time, a special attention is given to how the partnership and external interaction, especially between EU and NATO, are tailored to enhance and complement the national contributions in the field of resilience.

***Keywords**: CSDP; resilience; EUGS; Strategic Compass; PESCO; EDF; EPF.*

Introduction

Although resilience is one of the concepts widely circulated in recent years, precedents for its use at EU level date back to 2012, when the European Commission adopted the Communication on resilience (COM(2012)586). It was based on the experience of food crises in Africa in the first decade of the twenty-first century. Consequently, the European Commission's approach was directed towards managing this type of vulnerability by strengthening resilience through the optimisation of its own external action to support developing states. Although it can be seen as a one-off issue, the Communication provided the framework for defining the parameters of the EU's overall positioning towards resilience issues. Thus, this moment is linked to the emergence of the first definition, agreed at EU level, of resilience referring to "the capacity of an individual, family, community, country or region to cope, adapt and recover quickly from trials or shocks" (p. 5).

The implementation of a response formula for the two dimensions – the capacity to withstand shocks and the ability to recover – could only be achieved through a multidisciplinary strategy meant to reduce the risks of crises, doubled by the adaptation of internal mechanisms in different geographical perimeters. From this perspective, strengthening resilience was placed, as an actionable area, at the intersection of humanitarian and development assistance. The time perspective associated with this approach envisaged a long-term commitment to building resilience, structured on the basis of the bottom-up approach. Basically, it was envisaged to empower the entire set of policies and instruments from which a state benefited, thus strengthening resilience as an integrated approach of them. The generic structure of the EU's response to building resilience included:

− crisis anticipation and risk assessment, with a focus on reducing vulnerabilities at local and institutional level to enable them to be better prepared to mitigate negative effects, as well as to structure an effective response to incidents having natural causes;

− prevention and preparedness aimed at structural, long-term/sustainable approach to the causes that determine the threats to the resilience and, subsequently, states' vulnerabilities; this also resulted in the priority given to integration;

− strengthen the crisis response, where major attention was paid to inter-regional coordination and the external assistance process. It was also considered the importance of defining strategic priorities in strengthening immediate/short-term resilience (early recovery), as well as in a longer temporal situation. Given the overall profile of the EU's commitment, it was envisaged to connect European policies, especially the Common Security and Defence Policy (CSDP), for crisis situations that could mark the conditions for implementing the cooperation agenda with the affected states.

The principles and courses of action submitted by the European Commission have been politically validated by the Conclusions adopted at EU Council level on resilience (Council Conclusions on resilience, 2013). The Council's approach gave additional political input to the EU's approach to resilience, stressing the importance of linking policy dialogue with development and humanitarian processes/initiatives. Building on the milestones of the Commission Communication, the EU took into consideration a wide range of situations which helped to consolidate resilience, such as: conflicts, insecurity, weak democratic governance, economic shocks, natural accidents, climate change. Thus, the conceptual platform submitted by the Commission as regards the principles underpinning the EU approach was formalized (GAERC, 2013, pg. 3-4) starting from the following principles:

− the primary responsibility of governments in developing resilience;

− convergence of vision between the different national actors involved, as well as between EU and Member States;

− medium and long-term approaches to humanitarian and development planning; deepening bilateral and multilateral cooperation in implementing the resilience-building agenda;

− promoting an active approach to specific aspects of conflict situations, in particular as regards the humanitarian, development and policy dialogue dimensions;

− the need to invest in local capacity, while developing regional potential and constant dialogue with different local entities;

− commitment to long-term development of resilience;

− ensuring the implementation of the gender perspective;

− focused approach to vulnerabilities;

− supporting sustainable solutions among the refugee population;
− promoting transparency and efficiency in implementing resilience, including from the perspective of developing measurement tools.

The implementation of these principles was to be achieved through an Action Plan that outlines the features of EU approach in terms of the central role of states in implementing measures regarding: strengthening resilience, topics of interest – civilian population; promoting the action matrix bringing together coherence – complementarity – coordination – continuity. Under these conceptual auspices, the advanced priorities for the EU's contribution in support of other states were the following: EU support for the development and implementation of national and regional approaches to resilience, internal capacity and partnership; innovation, learning and advice; resilience support methodology and tools (Action Plan for Resilience , 2013).

2. Strategic Approach to Resilience

Undoubtedly, the Commission's Communication and its political validation were the cornerstones of structuring EU's approach to resilience. Already at this stage, however, the focus on addressing resilience in the context of EU's external action in relation to partner states is distinguished. The premise of this approach was that developments in the immediate vicinity of the EU were likely to generate disruptive effects on the security of Member States. Thus, it became an immediate need to strengthen the EU's support capacity, especially when the capacity of most states in the immediate vicinity was particularly fragile to face major challenges to their own stability.

At the same time, the ownership of the European Commission, at this stage, outlined specific features characterized by standardization of support formulas and having a pronounced economic character. From this perspective, the Commission's Communication is a specialized and initial element in the comprehensive definition of resilience at EU level. In June 2016, the defining moment was represented by the adoption of the Global Strategy of the European Union (EUGS). At its level, resilience was one of the main elements promoted in association with the EU's global profile in the area of security and defence. The EUGS also offers a bivalent perspective on resilience, centered both on the internal component, at EU level, and on the external action of the European body (EUGS 2016, p. 4).

In this respect, strengthening resilience in the European context has added extra valences to the existing framework at the time of the EUGS emergence. The dominant note of how this objective was designed concerned both the dimension of democratic values and principles, as well as the security note in which instruments and policies developed at EU level would be used to build resilience (e.g., cybersecurity and

countering hybrid threats). From the perspective of external interaction, resilience was projected as one of the priorities of the EU's external action, focusing on the dimension of the two vicinities and approaching both state and societal level. Within this framework, EU will support the different courses of action by focusing efforts and support for these states in key areas (governmental, economic, climate, energy). The EUGS also advances a new interpretation of resilience as a concept extended from the individual to society as a whole. The existing conditionality between security – prosperity and democracy – resilience is the essence of this approach in which the EU must promote and invest sustainably in the resilience of states and societies. The geographical perspective is extensive, including states "from Central Asia to the south of Central Africa" (EUGS, 2016, p. 23). At the same time, the concrete ways to promote this objective cover a wide range of formulas, including both the criteria associated with the enlargement process and the cooperation policy within the European Neighborhood Policy (ENP), as well as adapted policies aimed at responding to deficits and the critical situation at local level, such as: fight against terrorism, corruption, organized crime and the protection of human rights. To these are added the local ownership in terms of justice reform, security and defence sector, respectively the construction of relevant capacities at state level. In this context, CSDP is individualized as an instrument with the potential to deliver tangible results in terms of partner states' capacity to ensure the necessary security conditions for the deployment of assistance programs on the ground.

Within the level of ambition promoted by the EUGS as reflecting the EU's global profile in the area of security and defence, resilience has been a substantial component associated with partner capacity building. The separate note refers to the systematic approach of this area for states that are in the process of recovery in a post-conflict context or of increased instability. This includes the role of CSDP to provide assistance and expertise to strengthen partner states' national capacities and to provide expertise and assistance in countering hybrid threats, including cybersecurity, strategic communication and border security. Also, responding to the bivalent internal-external perspective, the issue of resilience is also addressed in correlation with the EU's internal potential to face security challenges and risks, especially in terms of protection of critical networks and infrastructure, supply chain security, promotion of technological endowment and investments in defence (Implementation Plan on Security and Defence, p. 3).

The structured and, equally, comprehensive vision promoted at EU level through the Global Strategy and its implementation plan placed the issue of resilience on strategic coordinates. One of the facets that the EUGS promoted undoubtedly concerned the security and defence dimension of the resilience-building effort. This approach encompassed both the operational dimension and the launch of concrete capability initiatives and projects. At the same time, concern about the security aspects

of resilience was manifested in the context of the security environment degradation following the Russian invasion and occupation of the Crimean Peninsula. On these coordinates, EU's efforts in the field of resilience were advanced in a much broader manner than before, including the options through which European cooperation in the field of security and defence could respond to these concerns, both internally and externally.

The EUGS's course of action on the importance of resilience in the context of EU external action was deepened in a new Communication adopted in June 2017. The characteristic of the new approach was to promote an integrated approach. Under the auspices of new political directions and structured as a long-term commitment. Without excluding the practical dimension of cooperation with partner states, the deepening of the bipolar perspective was envisaged, the internal dimension of resilience being addressed more carefully, in a complementary manner with external action approaches.

It can be argued on an attempt to extend the conceptual framework for reporting the EU to the issue of resilience. Practically, it concerns another phase of the evolutionary process that was initiated in 2012 when the Commission Communication, based on a particular evolution in the field of food security, placed resilience in a context relatively limited to the capacity to withstand shocks. Contrary to this approach, EUGS has projected a more comprehensive perspective, extending the issue of resilience to society as a whole, with obvious political vocations linked to democratic rights and foundations. In the context of the realities determined by the emergence of the EUGS and, subsequently, of the adoption of an EU level of ambition in the field of security and defence, the new Communication also aimed to adjust the conceptual framework – practically to the new realities generated by the EU's profile as a global actor. Thus, we can talk about the reassessment of resilience as a foreign and security policy instrument, as well as an essential parameter for calibrating the efforts of Member States and the Union to strengthen the stability and security of their own area. On these coordinates, resilience becomes a strategic priority structured, thus, on all levels and much closer to the capacity of adequate functioning of the state.

In terms of internal resilience, it can be advanced the idea of designing it as a deterrent formula, meant to prevent coercive or aggressive actions from the external environment. Within this perspective, EU's capacity to anticipate and, subsequently, initiate proactive political and operational actions was a priority direction (JOIN(2017)21 final, p. 15). In order to achieve the EU's capacity to optimally manage the challenges to internal resilience, concrete dimensions of action were envisaged to:

− Resilience against hybrid threats – with priority in strengthening critical infrastructure protection, diversifying energy sources and developing defence capabilities. The potential for connection between Member States was to be one

of the strategic priorities of this area, contributing to deepening integration and interconnection at EU level;

− Cybersecurity – through internal reinforcement of communication services and networks within the EU as well as EU external support to the UN, including cross-border cooperation;

− Strategic communication – focused on increasing the resilience of EU population to disinformation, as well as increasing EU's capacity to manage the challenges of this area on geographical coordinates;

− Countering terrorism and violent extremism – in addition to domestic aspects of detecting, preventing and exterminate terrorist organizations and sources of funding, partnership development and bilateral dialogue were envisaged;

− Strengthen the security of critical transport infrastructure – including in terms of developing interaction and cooperation with non-EU states to reduce the threat in this area. From an internal perspective, internal capacity development, strategic awareness, IT tools are considered; increasing the role of the police and judiciary;

− Cooperation between EU and other multinational organizations.

3. Strategic Compass and a New Perspective on Resilience

The adoption of this document is also placed in the context created by the European Union Global Strategy aimed at developing more ambitious European cooperation in the field of security and defence. On this line of action, the first discussions regarding the rationale for adopting a new strategic level document converged towards giving particular importance to the issue of resilience identified as one of the main directions of action that European cooperation had to pursue. As is known, the Strategic Compass was adopted at the Foreign Affairs Council meeting on March 21st, 2022. The peculiarity of the moment was accentuated by the fact that it took place less than a month after the launch of Russian aggression against Ukraine. The impact of aggression would be reflected intensely in terms of valuing the importance of resilience, both in terms of external action and in terms of internal capacity at Member State level to face security challenges to their resilience.

Unlike other documents and approaches used at European level in the development of this area, the Strategic Compass places resilience much closer to the internal security of the European Union. Clearly, this course of action derives from the dramatic acuity of the war in Ukraine and a relatively insufficient level of coagulation of some options to ensure internal security at European level. Equally, the perspective advanced by the Compass in terms of promoting resilience can be regarded as an upper stage in the development of the European agenda, structured by deepening the directions of action generated by the EUGS, while adapting the EU's level of ambition in crisis management to the realities generated by the war in Ukraine.

In terms of continuity with advanced elements through the EUGS, the resilience approach at Strategic Compass level provides concrete directions for implementation, as is the case with the development of tools to combat cyber and hybrid threats. Capacity building at European level is also envisaged in terms of resilience in managing interference and manipulation. The dominant note projected by the new document is strongly anchored in the idea of internal capacity building in these areas, with emphasis on developing the potential for anticipation and early warning on the imminence of aggressive actions. Equally, the functional parameters of the envisaged toolkit target both the conceptual dimension and the capacity to identify, deter and defend actions in the cyber and hybrid domains, profiled in an integrated matrix, supported by an efficient communication system. The relationship of these objectives with the operational dimension of the EU developed under the CSDP aegis was likely to provide novelty elements that the Strategic Compass brought in the context of European cooperation in the field.

Based on the need to coagulate a concrete action profile in the field of resilience, the creation of that type of relevant capabilities was envisaged to strengthen the posture of operational commitments regarding hybrid and cyber threats. The empowerment of initiatives developed in the field of capabilities such as the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) represented a concrete dimension through which the field of resilience was translated to the level of practical cooperation projects with the participation of Member States (Strategic Compas, 2022, p. 22). At the same time, addressing the operational development potential in cyber and hybrid management was also reflected in the development of specialized teams that could be engaged in support of Member States.

The internal dimension of resilience has been placed in a higher matrix in terms of ambition juxtaposed to the EU's global security profile. The main element concerned the objective of ensuring the Union's access to strategic areas (maritime – air – space), resilience being seen from the perspective of strengthening the capacity to promote EU interests at global level. The disclaimer of these objectives aimed at adapted implementation, including both a component to complement the conceptual-doctrinal framework and concrete aspects of implementation in an institutional context shared between the European Commission and EU Council. The space policy, with direct applicability in the field of security and defence, represents one of the distinct directions advanced by the Strategic Compass, both from the perspective of situational monitoring, the development of necessary capabilities, and reaction potential (Strategic Compass, 2022, p. 24).

On March 10th, 2023, building on the priorities advanced through the Compass, the European Commission and the High Representative for Foreign Affairs and

Security Policy presented a Communication on the EU Space Strategy in the area of security and defence. At this level, the issue of resilience was seen as a priority in terms of ensuring EU access to the spatial dimension. Thus, resilience translates into achieving the autonomous capacity of the European Union to act autonomously and, subsequently, to ensure the protection of its own facilities and capabilities. The connection of this approach with the security and defence dimension is validated by promoting an active posture across the entire set of space systems and services developed by the EU (JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the European Union Space Strategy for Security and Defence, p. 7). It should be mentioned that this approach represents a premiere for the European Union, being the first strategic vision on the use of space, including through direct applicability in the field of security and defense. The priority given to resilience is also found at the level of integrating the functionalities foreseen for the space approach, together with those related to cyber and hybrid dimensions, within a matrix for managing asymmetric challenges and threats (JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the European Union Space Strategy for Security and Defence, p. 9).

Equally, the dimension of partnerships and relations with third states that the Strategic Compass addresses in the context of developing resilience cannot be excluded from discussion. Together with the operational arm of CSDP, it is the building block of external resilience that includes elements associated with cooperation between the EU and partner states in the two neighborhoods. Basically, the Strategic Compass represents a new opportunity to explicitly reconfirm the interest in continuing EU's commitment in supporting and developing the resilience of partner states. The operationalization of this objective mainly concerns the tools developed in the context of external action and, subsequently, CSDP. On the same coordinates of the manifest interest in deepening cooperation in the field of resilience is placed the capitalization of the partnership formulas developed by the EU in relation to other international organizations. As with other aspects, the provisions of the two EU-NATO Declarations, adopted in 2016 and 2018, were milestones on how to deepen cooperation in the field of resilience. On these coordinates, the framework provided by the two documents included a consistent set of actions and cooperation projects in the cyber, hybrid, CBRN resilience, exercise coordination, strategic communication as well as in terms of harmonizing the approaches of the two organizations in strengthening the resilience of partner states. The focus on the resilience component of EU-NATO cooperation was one of the elements advanced through the Third Declaration signed by both organizations in January 2023 (EU-NATO Declaration, 2023).

4. Dimensions of Resilience Implementation in the Context of European Security and Defence Cooperation

Building on the milestones advanced in the Commission's 2017 Communication, four components were envisaged for the external dimension covering and applicability of CSDP to be included in the external action to:

− improving analytical capacity and disseminating risk analysis at national and regional level, as well as interaction at Council level to ensure policy dialogue and programming of assistance;

− introduction of a dynamic system for monitoring external pressures and faster political and diplomatic response;

− mainstreaming resilience in external action planning and financing;

− development of international and practical resilience policy (Strategic Approach to Resilience, 2017, p. 5).

At the same time, the strategic paradigm agreed by the EUGS regarding the applicability of the concept of resilience in a "the whole of society" approach is completed by the dimension of basic functionalities and mechanisms of state functioning. From this perspective, the contribution of external action and subsequent CSDP was intended to ensure a resilient environment in EU's vicinity while contributing to overall resilience within the Union (JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL A Strategic Approach to Resilience in the EU's external action). In this regard, the role of European cooperation in security and defence can be seen as backdating the formalization interval of EU's priorities in the field of resilience. Thus, elements associated with support to neighborhood states for resilience building can be identified in terms of mandates set for crisis management missions and operations that the EU will carry out from 2003.

They also cover both military and civilian commitments. Even if for the period prior to adoption of the EUGS, resilience was not explicitly mentioned as one of the main goals, the objectives of the missions and operations carried out between 2003 and 2017 support the strengthening of the resilience of EU-supported states. The most relevant dimension in this direction is support for security sector reform. This element is also common to the commitments in the Western Balkans, launched in the context of restoring the security climate after the outbreak of conflicts in the former Yugoslav area. On these coordinates is placed the Civilian Police Mission of Bosnia and Herzegovina (EUPM BiH) (2002/210/CFSP), respectively the Althea military mission deployed since December 2004 in the same geographical perimeter and, last but not least, the missions in North Macedonia. Subsequently, the typology for structuring support to state institutions in the EU's neighborhoods has diversified substantially, including complex formulas of assistance to the armed forces and

police in an extended context of the security sector reform process, as in the case of missions in Africa (Central African Republic, DR Congo, Sahel - Mali and Niger, Somalia, Mozambique). On these coordinates, there are also a series of missions targeting niche/specialized support on the reform component of the legal system and in the field of human rights (Georgia, Iraq, North Macedonia).

The importance of resilience in connection with EU's operational commitments in crisis management has benefited from an additional validation in the security context affected by Russia's aggression against Ukraine. In view of the marked degradation in the security environment in Europe, the focus on resilience in terms of how EU can contribute to strengthening the capacity of partner states has gained significant emphasis. In terms of EU-led operational commitments, this approach is best reflected in the context of the Partnership Mission launched by the EU to the Republic of Moldova at the end of April 2023. The main objective of this operational approach aims to strengthen the resilience of the security sector of this state in the field of crisis management and the capacity to combat hybrid threats, including cyber security and combating manipulation and external interference. The inventory of measures envisaged covers a wide range of possibilities for implementing EU support, ranging from identifying support needsin different areas to advising on the development of the security sector conceptual framework (2023/855).

In addition to the operational agenda, the implementation of resilience in the CSDP context is also manifested through the instruments developed in recent years, building on the provisions of the Lisbon Treaty. It was mentioned earlier capitalizing on the potential of cooperation formulas in the field of capabilities as an option to optimize operational commitments, to which is added the possibility of using financing instruments to support the reform processes of the armed forces in partner states. This is the context in which is placed the European Peace Facility (EPF), an instrument created in March 2021 as part of the process of reconfiguring external action instruments in support of the objectives of the EU Global Strategy. Obviously, the main direction aimed at streamlining the support provided by the European Union to partner states in both geographical neighborhoods. The distinctive character of the EPF is given precisely by the emphasis placed on defence issues, a trend set by the Treaty of Lisbon and, subsequently, by the EUGS. According to the functional parameters associated with the defence dimension at EU level, the EPF was structured on two components/pillars aimed at ensuring common costs related to military operations (pillar I), respectively financing assistance measures for the armed forces of partner states (pillar II).

At the level of the objectives set for the functioning of the EPF, the resilience of the states receiving EU support was one of the priorities in terms of strengthening their military and defence capabilities ((CFSP) 2021/509 , p. 46). Resilience is also approached from a broad perspective through the possibility for the EPF to support the

actions of regional and international organizations in the field of crisis management. The main way of implementing support is through assistance measures proposed by the High Representative for Foreign Affairs and Security Policy in cooperation with Member States and approved by the EU Council. The principles envisaged for defining these assistance measures shall cover:

− their consistency with the policies and objectives of EU's external action to strengthen peace, prevent conflicts and strengthen international security;

− compliance with EU law, EU policies and strategies and UN Security Council resolutions;

− compliance with the obligations of the Union and its members, in particular human rights and relevant legislation;

− taking into account the specific character of Member States' defence policy and not running counter to the security and defence interests of the Union and the Member States. − Beyond the operating reasons behind the EPF, this new instrument contributed to a much closer rapprochement between European defence cooperation and the dimension of EU external action. At the same time, the financing opportunity that EPF offers to partner states is a premiere in terms of predictability of financial support in the defence field. However, the EPF was built on the formal framework provided by the EU Treaty for regulating European defence cooperation, according to which such expenditure cannot be borne by the EU budget. From this perspective, the EPF budget was built outside the Multiannual Financial Framework 2021-2027, targeting a total financial envelope for the two pillars of EUR 5 billion, staggered for the mentioned period.

The assistance measures adopted by the EU between 2021 and 2022 targeted a number of states such as Somalia, Mali, Niger, Georgia, the Republic of Moldova, Ukraine, Bosnia and Herzegovina, as well as in support of African Union peacekeeping missions. Also, in the context of the war in Ukraine, triggered by Russia's aggression, the European Peace Facility is the main instrument through which the EU provides assistance to the Ukrainian armed forces, its level currently reaching approximately EUR 4.6 billion.

Conclusions

Although resilience is a relatively recent emergence in the landscape of European security and defence cooperation, within a short time it has become one of the essential milestones on the Common Security and Defence Policy agenda. This approach tends to be strengthened both conceptually and in reporting on practical steps to develop capabilities and allocate resources that match the focus on resilience.

As can be seen, the manner of deepening resilience in the context of CSDP is highly multidisciplinary, where both operational aspects and elements associated with

the capability agenda are found. In this equation, we cannot discuss a distinct path to resilience, the option taken at the European level being to associate this conceptual paradigm to the operating framework and objectives pursued in the context of CSDP. The approach within these parameters also explains the absence of a distinct level of ambition to ensure resilience in a security and defence context. However, the positive impact of corroborating resilience with the security and defence cooperation agenda cannot be overlooked, which contributes to strengthening the relevance of cooperation programs with different partners and third states and, subsequently, to substantial progress. In the same paradigm is positioned how resilience is reflected at the level of cooperation formulas developed by the European Union in relation to other international organizations. EU-NATO interaction is one of the courses of action with substantial development potential, all the more relevant from the perspective of strengthening convergence between these organizations.

Obviously, the emphasis placed on the external dimension of resilience is also dictated by the profile of European cooperation in the field of security and defence, whose directions of manifestation are, according to the provisions of the EU Treaty, exclusively external to the geographical space covered by the European Union. However, the realities of the security environment, culminating in Russia's aggression against Ukraine, bring to attention the importance of addressing resilience from the perspective of internal security and defence of the European Union. This trend has already gained consistency through the development of relevant EU tools in areas such as cyber defence, hybrid threats and space security, with significant interest from Member States to move in this direction.

BIBLIOGRAPHY:

Council of European Union.2002. JOINT ACTION of 11 March 2002 on the European Union Police Mission, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002E0210-20030317

European Union, 2012. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. The EU Approach to Resilience: Learning from Food Security Crises", https://www.eeas.europa.eu/sites/default/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf

General Affairs and External Relations Council. 2013. "Council Conclusions on EU Approach to Resilience", https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/137319.pdf European Commission. 2013. "*Action Plan for Resilience in Crisis Prone Countries, 2013-2020*", https://ec.europa.eu/echo/files/policies/resilience/com_2013_227_ap_crisis_ prone_countries_en.pdfEuropean Union. 2017. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE

COUNCIL. A Strategic Approach to Resilience in the EU's external action, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:21:FIN

European Union External Action Service. 2016. "Shared vision, common action. A stronger Europe : a global strategy for the European Union's foreign and security policy**",** https://op.europa.eu/en/publication-detail/-/publication/3eaae2cf-9ac5-11e6-868c-01aa75ed71a1

EU-NATO. 2016. "Joint Declaration by The President of The European Council, The President of the European Commission, and The Secretary General of the North Atlantic Treaty Organization", https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

Council of European Union. 2016. "Implementation Plan on Security and Defence", https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf

European Union. 2017. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. A Strategic Approach to Resilience in the EU's external action", https://www.eeas.europa.eu/sites/default/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf

EU-NATO. 2018. "Joint Declaration on EU-NATO Cooperation by The President of the European Council, The President of the European Commission, and The Secretary General of the North Atlantic Treaty Organization", https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

Council of European Union. 2021. COUNCIL DECISION (CFSP) 2021/509 of 22 March 2021 establishing a European Peace Facility, and repealing Decision (CFSP) 2015/528, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0509

Council of the European Union. 2022. "A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security", https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

EU-NATO. 2023. "Joint Declaration on EU-NATO Cooperation", https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/

European Union. 2023. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. European Union Space Strategy for Security and Defence", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0009

Council of the European Union.2023. COUNCIL DECISION (CFSP) 2023/855 of 24 April 2023 on a European Union Partnership Mission in Moldova (EUPM Moldova), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023D0855

DOI: 10.53477/1842-9904-23-10

COMPLEX SECURITY CHALLENGES – COMPLEX RESPONSES

Endre SZŰCS PhD*
Miklós SZAKALI**

Due to the increasing complexity of the security challenges, it is necessary to change the approach and understand security in a much more complex way than before. We consider it even more important to provide the capabilities needed to meet complex security challenges than changing the theoretical approach. Without providing the necessary capabilities, we will not have a chance to prevent and manage complex security challenges.

In the present article, we examine the possibility to ensure complex military and civilian capabilities corresponding to complex security challenges. Also, it is being considered the development and the usability of the defence planning system, generated and used by the military, in order to provide civilian capabilities. Furthermore, we propose to set a parallel structure for military and civilian capability development to provide adequate complex capabilities for complex challenges.

Keywords*: complex security; security challenge; defence planning; national security strategy; international security; international security structure; critical infrastructure.*

**** Endre SZŰCS, PhD, is Supervisor and Senior Lecturer of the Doctoral School of Security Studies at Óbuda University, Budapest, Hungary. E-mail: szendre63@gmail.com***
*****Lieutenant colonel Miklós SZAKALI is a Senior Analyst and Planner within the Ministry of Defence, and a PhD Candidate in the field of investigation of the interactions between security and defence planning within the Doctoral School of Security Studies at Óbuda University, Budapest, Hungary. E-mail: mszakali@hotmail.com***

Introduction

Throughout history, security has been identified with military security by many branches of science, politics and common knowledge alike. Based on this approach the main driver of security was to avoid armed conflicts and war, almost everything had to promote this policy. The international security institutional system and states' security structures were also established with focus on the management of the military field of security. Accordingly, every effort was made to provide the necessary military forces and capabilities essential for military security.

However, new types of non-military security challenges are increasingly gaining ground in our time. If we consider the basic problems of our days, the COVID-19 pandemic, the effects of climate change, and the extremely rapid development of technology, we can experience that they have already determined our security and expect to have an even stronger impact on it in the future. These challenges do not only cause security risks or dangers in the security dimension, but rather appear in a complex way and have a significant impact on several areas of security. One must admit that neither the international security institutional system, which mainly focuses on military security, nor the states are prepared to deal with comprehensive security challenges. Certainly, international security organizations are trying to adapt to the current challenges and help in the prevention and management of new types of security challenges. However, they lack the capabilities, resources and in many cases, the authorization in dealing with the roots of the problems and thereby, real crisis management. Beside the field of military security, there is no scientifically based method or procedure for capability development and crisis management appearing in any other non-military dimension of security. This statement is even more exact with regard to complex security challenges touching numerous dimensions of security. However, considering the nature of potential security challenges covering several areas, it is not possible to develop specific capabilities to deal with each challenge due to the limited availability of resources and the time-consuming nature of capability development process. Therefore, a solution must be found which, although not specific, can ensure the survival of a country and its population and the management of the emerging crisis by maintaining and developing vital capabilities in the long term. A tool already developed and applied successfully in the field of military security, which is defence planning, can significantly help, since this tool was of crucial importance in security and peace preservation during and after the Cold War, including current changes in the security environment.

1. Defence Planning and Changing Challenges

The 20th century security concept was also reflected after World War II when the international security institutional system (UN, NATO, EU, etc.) was established.

The basic task of the institutional system was to prevent the outbreak and escalation of armed conflicts, thereby avoiding a new war. (UN, un.org 1945) (EU, european-union.europa.eu 1945-59) Therefore, the international security institutions developed their own specific policies, capabilities and assets to fulfil this determinate objective. In the security environment defined by the military confrontation, it became obvious that only those organizations were important enough and could achieve real results in maintaining security, which had real military strength and capabilities. (NATO 1949) Organizations without effective military power became weightless and had no influence in security issues.

On the Western side, the system of defence planning was one of the decisive tools that ensured the West's military strength and capabilities during and after the Cold War, in the midst of multilateral challenges. At the beginning of the Cold War, NATO's military and civilian planners were not yet thinking in terms of long-term forward-looking planning. In April 1951, NATO forces were limited to twelve land divisions, 400 fighter planes. (Bitzinger 1989)

After the German capitulation, the 4,720,000 Western forces were reduced to only 879,000 troops. The Soviet Union, on the other hand, maintained its wartime armed forces of 4 million gaining an obvious superiority over the West. (Bitzinger 1989) The emerging military situation forced the Western planners to balance the Soviet military superiority as soon as possible, which also meant averting a potential military conflict.

When they achieved this short term and very demanding aim, the lessons had been learned, namely the "reactive mode" (force and capability balancing) should be avoided. They recognized that a forced situation where they always had to follow in their opponent's footsteps required great effort and resources in the short term, and in case of failure, the opponent could gain advantage that might upset the military balance and increase the risk of armed conflict. This realization was followed by the forward-looking planning of military forces and capabilities for an increasingly longer term. Only such long term forward-looking planning could continuously provide the necessary military forces and capabilities for maintaining the regional security and ensure the advantage, ultimately, the victory of the Western bloc in the Cold War.

It became general opinion that relying on the economic advantage of the West did not make it easier to overcome the military power of the Eastern bloc. In our view, given the recognition of the West's economic advantage, the role of defence planning should be highlighted. The Western planners recognized the fact that it is not enough to spend more and more resources on the development of military forces and capabilities, it is not enough to "pour money into defence". Even the richest country was not and is not currently in a position to spend the maximum of resources on every segment of defence (maintenance, capability development, operations, etc.).

Therefore, "smart spending" became particularly important, which determined the proportion of resources to be spent on the main activities, maintenance, operations and capability development, as well as provided the resources for the implementation of the most important objectives (priorities).

Without this theoretical approach, there was a risk of wasting resources with multiple negative consequences, i.e. resources ran out and usable, advanced forces and capabilities were not created. All these considerations made necessary the application and development of defence planning. In the development of defence planning process one of the cornerstones was the development of the US Planning-Programming-Budgeting System (hereinafter: PPBS) (Britannica 1961) (Tulkoff-Gordon-Dubin-Hinkle. 2010), which brought the political objectives, military capabilities, resources and time constraints to the same platform and dealt with them based on their interrelations. Building all of this on a short, medium and long term time horizon provided the necessary foresight and capability development to meet expected security challenges. The system was adapted by NATO and its member states and further developed according to their goals and characteristics. (Stojkovic-Dahl 2007) The system of defence planning proved to be successful during the Cold War and, then, also responded in a flexible manner to the challenges of the changed and more demanding security environment following the Cold War. It has been able to provide adequate forces and capabilities for crisis management, counter-terrorism and anti-piracy operations and currently for the deterrence and defence strategy of the West to prevent the spill over of the Russian-Ukrainian war.

The 21st century has passed beyond the exclusive nature of military security challenges and complex security challenges has gained ground and became decisive. Nowadays, there is no security challenge that affects one security dimension exclusively, and does not spread to other sectors of security (political, economic, societal, military and environmental) (Buzan-Waever-Wilde 1997), turning it into a comprehensive challenge or crisis. (NATO-ACT 2017) Considering the recent security events, it became clear that these complex security challenges cannot be managed using the old instruments of international security institutions. Certainly, they do everything possible to support countries in crisis situations, according to their mandate and instrumental possibilities, however they are unable to remedy the root of the problems. They were not able to prevent and stop the COVID-19 pandemic, or to prevent and manage the development and effects of climate change, illegal mass migration, water shortages, energy crisis, food crisis, or prevent the outbreak and escalation of armed conflicts (Azeri-Armenian, Russian-Ukrainian, and Turkish- Syrian).

Next, we would like to illustrate the change and complexity of security challenges by highlighting the following two examples. Terrorism is not a new phenomenon, but becoming transnational, it has created a new situation and a complex global

challenge that is not limited to separate states or regions. (Brown 2022) . Using the results of digitalization and technological developments makes the danger of terrorism grow constantly and expands all dimensions of security. With their attacks, they create mistrust in state institutions, and the population questions the government's intentions and the effectiveness of the security system to protect citizens. The effects of terrorist attacks may lead to general discontent that can culminate in a social explosion, ultimately even to a civil war. As we can see, common crimes against societal security (explosions, attacks on critical infrastructure, etc.) have an impact on the political, economic, military and environmental dimensions of security as well. Therefore, we can assess the prevention and treatment of terrorism as not primarily a military task, however it can be achieved by a comprehensive solution.

A typical 21st century challenge is the cyber threat. It is one of the most dangerous current security challenges, which can be used in many ways, independently and as part of other operations (information, psychological, hybrid, etc.). It poses a particular danger because the attack can remain unnoticed even for a long time since its effect is not manifested in spectacular destructions or casualties. A cyber-attack can be aimed at one or all of the security dimensions, causing huge damage to the given sector or to the whole country. Think of the presidential election, a vital political event for the US, but also decisive for the world, which was already accompanied by international tension in 2016 due to the Russian cyber-attack. According to experts, the Russian President gave direct instructions to the St. Petersburg Internet Analysis Agency to influence US public opinion. (National Intelligence Council 2021) In addition to political influence, economic benefit and destruction have also become the targets of cyber activities. In May 2021, the East Coast oil company USA Colonial Pipeline was hacked causing significant supply shortages for the economy and the public as well. The company used to deliver 2.5 million barrels per day, 45 percent of the fuel supply of the East Coast. The shortage persisted for many days and the USA had to declare an emergency situation to ease the crises. (Manageengine 2021) The incident highlights that cyber-attacks pose an increasing threat not only to the economy and the politics, but also to the elements of the national critical infrastructure, which provide the basis for the daily life of society.

We have selected the two examples above because, based on their connections, one can get an overall picture of the complexity of security challenges. Terrorism itself is a serious threat to security, this is well illustrated by the example of ISIS, which exercised state-like functions and extended its power to all dimensions of security. (Besenyő 2019) In this way, it has become a decisive player from the individuals and smaller communities level to country and region level. The impact of terrorism on security is further enhanced by access to the results of advanced technology, such as the use of the Internet, cyberspace and digitalization. All of these possibilities significantly eases the planning, organization and execution of terrorist

activities, increasing the effectiveness and danger of terrorism. This symbiosis is very well presented in the article "Hezbollah and the Internet in the Twenty-First Century" (Besenyő-Gulyás-Trifunovic 2023) and points out to the need for a comprehensive response to security challenges even more understandable. All of it does not mean that the military dimension of security will lose its importance. Based on experiences in Afghanistan, Iraq, Mali and other hotspots, military capabilities remain indispensable and should be further developed, however we have to admit that alone this is not enough to solve complex challenges.

It became obvious that the countries alone have to cope with security challenges and crises with relatively little international support, at least in the beginning. It is also clear that it is not possible to develop separate capabilities to deal with each of the diverse and complex security challenges. The limited availability of resources and time constraints do not allow us to counterbalance each element of complex challenges with distinct forces and capabilities. Therefore, a strong general base should be established to provide primary resistance, defensive line and provide time and opportunity for developing specific capabilities. We consider critical infrastructure as the most suitable assets for a general base to further build on, since their basic purpose is to provide the necessary products and services for social and individual survival. The importance of critical infrastructure is clearly shown by the fact that during COVID-19 pandemic, several countries (Italy, Hungary, Spain, etc.) have ordered and secured the operation of critical infrastructure under all circumstances, involving the armed forces and the police. We can also see the decisive role of critical infrastructure in the Russian-Ukrainian war, where the Russia is deliberately attacking them, trying to make the Ukrainians' life unbearable and, in this way, break the resistance of defence.

2. The Possibilities of Defence Planning in the Development of Civilian Capabilities

Bearing in mind the facts and considerations above, the questions which arise would be: Is it possible to develop forces and capabilities that can meet the requirements of comprehensive security challenges? Can the defence planning system developed for the military component of security be applied to provide complex capabilities? Where and what changes need to be made for the defence planning system to be suitable for the development of civilian capabilities? These questions must be asked at the national level by the authorities of each country, since at the international level both NATO and EU made reference to the development of resilience (civilian capabilities) as a national responsibility (NATO, nato.int 2016) (Lasconjarias 2017) (EU, commission.europa.eu 2020).

Our study aims at searching and providing an answer to the afore questions, i.e. whether the defence planning system can be applied to the development of critical infrastructure and, thus, civilian capabilities. After examining different defence planning models, we consider NATO's defence planning model and procedure a possible basis of our investigation. It is a general model based on the above-mentioned PPBS principles that harmonizes the national defence planning models based on similar grounds, thus it has a sort of integrating and synthesizing function, which makes it suitable for the intended purpose.

NATO Defence Planning Process (hereinafter: NDPP) follows a four-year cycle and sets short, medium and long term capability development goals for the Alliance and, thus, also for the member states. However, the NDPP focuses on the short and medium term. Short term planning horizon includes 1-6 years, medium term 7-19 years and long term 19+ years. (NATO, nato.int 2022)

Figure no. 1: The NATO Defence Planning Process
(NATO, nato.int 2022)

The main steps of the NDPP:
1. Political Guidance;
2. Determine Requirements;
3. Apportion Requirements and Set Targets;
4. Facilitate Implementation;
5. Review Results.

The planning process is politically driven, since the security challenges and planning priorities for the planning period are initially defined. With this step the political leadership acknowledges and assumes responsibility for the fact that it is not possible to provide a complete response to all challenges and that even with the

most careful planning, some security risks will exist and politics must take them. It is also a political obligation to provide the necessary resources to achieve the defined objectives. Aside from the political aspect, the military side also plays a decisive role in the process, given that the military establishment "translates" political objectives into military forces and capabilities. Military expertise informs us of the quantitative, qualitative and readiness requirements of the necessary military forces and capabilities, by which the given objectives can be achieved, such as the collective deterrence and defence of the Euro-Atlantic region.

We have concluded that the theoretical approach and structure of the defence planning system provide the possibility to use it for civilian capability development. Following the process of the NDPP, the political guidelines should be translated into civilian capabilities. Adapting the military part of the process, civil professionals must determine the civil forces and capabilities and its related quantitative and qualitative requirements to ensure the implementation of the political will and the achievement of the set goals. To this end, the key issue is the professional implementation of step number 2, where this translation takes place and civilian capabilities are defined with all the necessary parameters. However, this is a complex and difficult task requiring great expertise and experience. The implementation of this task requires a team of experts who are aware of the expected consequences of potential military and non-military security challenges and their civilian capability requirements. Assessing all of the requirements should provide them with the ability to determine the necessary civil capabilities and identify those elements of the critical infrastructure that need to be developed. We do not see the need to make any differences in the structure and the sequence of the further steps of the planning procedure. The basic function of the steps should remain as it is in the present, however, their content may change according to the specifications of the planned domain. For instance, step number 3 includes the allocation of the capability development goals to the competent governmental portfolios and private sectors. There are no changes in the function of the step no. 4, dedicated to the capability development. In this phase plans become reality, it will turn out that our plans and calculations were correct or not and the planned capabilities are achievable or not. The final step of the process is the feedback, the review process, where we have to face our positive and negative results and continue the journey we started or make corrections. The aim is the objective analysis and assessment of our entire planning and implementation activities, otherwise we could get lost in this very difficult and complex process.

We should be aware that capability development is not a short term process. It usually takes about 6-10 years for a capability to become fully operational since it includes the provision of infrastructure, human resources, legal, financial and professional elements, as well as the developing, testing and introductory procedures.

In our opinion, DOTMLPFI[1] (NATO, The NATO Defence Planning Process 2016) system established by NATO for military capability development can also be adapted for civilian capabilities, this also helps to achieve usable capabilities. Taking all of it into consideration we found out that the planning objectives and directions should be defined, at least, for medium and long term, if it is possible, and the resources and other necessary conditions for implementation must be fixed in those plans as well.

For medium and long term capability development plans, especially with regard to critical infrastructure that includes several governmental portfolios, private sectors and sub-sectors, a well-coordinated work on concept and strategy development is essential. It might be useful to introduce the linkage between strategies and capability development process using our national (Hungarian) practice on the hierarchy of strategic documents. The comprehensive National Security Strategy (Government, honvedelem.hu 2020) is the highest policy document that identifies the main challenges, risks and threats and defines those elements essential for their prevention and management. This strategy also defines the priorities of national security and the main directions of capability development.

This is followed by the development of the strategy for each governmental portfolio or sector. It defines the expected main sources of security threats, risks and challenges, which must be countered with the sector's instruments and to this end, it sets the sector's main tasks and directions of capability development. These tasks and directions for capability development are planned in the medium and long term plans of the sector with resource allocation and deadline. However, we found that only some governmental sectors fulfil the obligation and prepare its own strategy related to the National Security Strategy. In many cases the sector-specific strategies are not in line with the National Security Strategy's requirements. This means that there is no centrally managed work on comprehensive capability development that responds to the complex challenges identified by the National Security Strategy.

Currently, the defence sector is following the afore mentioned process and is developing its own strategy, the National Military Strategy (Government, defence. hu 2021) operating the defence planning system to provide military forces and capabilities in line with the National Security Strategy and NATO's requirements. However, the military forces and capabilities are not enough to cope with complex challenges. There is a need for a structured civilian capability development process similar to the military one.

In this difficult period, only a complex governmental approach can provide the capabilities that offer the opportunity to cope with comprehensive challenges. The military side cannot exist without civilian capabilities and the reverse is also true, they can only form together the "two sides of the security coin".

[1] DOTMLPFI - Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, Interoperability.

Therefore, we recommend the following structured approach to establish a national security planning system in order to provide military and civilian capabilities in an integrated manner.

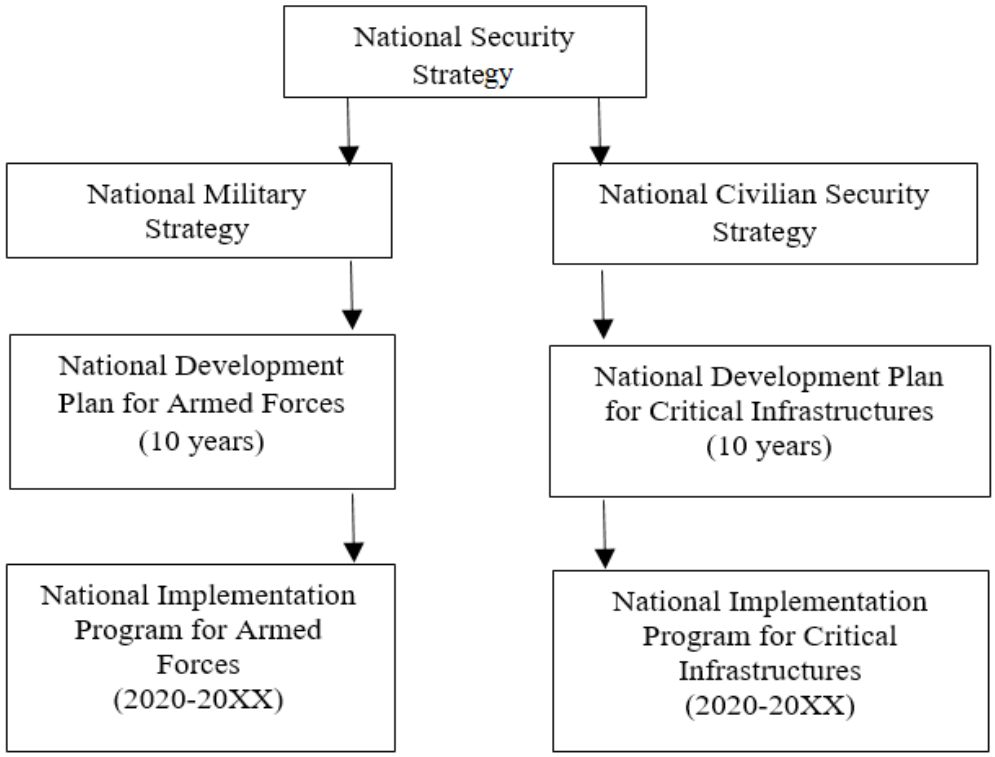

Figure no. 2: Possible structure of strategic planning and capability development on national level

In our view, the comprehensive interpretation of security includes the establishment of a joint structure for developing military and civilian capabilities in a harmonised manner to answer complex challenges. It would cost-effectively ensure the unity of efforts across priorities, avoiding duplication and overlap in capability development. It is our belief that the application of the defence planning system for the development of civilian capabilities would represent a significant step in answering complex security challenges.

Further research and experiments are necessary for the establishment and smooth operation of the integrated national security planning system, taking into account the differences and peculiarities of the civil sectors, but it is our strong belief that this idea should be continued and promoted.

Conclusions

Considering the complex and ever deteriorating security environment, there is a need to change our approach attitude to managing security challenges. We need to understand that the military and non-military security dimensions must be considered in equal measure, since both make up the whole of security. All of this must be reviewed in terms of the authority and tasks of international organizations involved in security matters, since nations received little help in managing recent crises.

We also consider necessary to follow a broader interpretation of security and to approach the security dimensions comprehensively on national level. As part of the security establishment, non-military dimensions should be integrated in the national security planning system on national level and the planning system of defence dimension is to be used as a common approach to develop the necessary capabilities.

It is obvious that we cannot counter complex security challenges by developing specific capabilities that respond to each element of a complex challenge because of the limited availability of resources and time constraints. There is a need for a comprehensive general base that ensures the availability of basic capabilities and provides time and opportunities for specific capability development in case of crises situation. In our view, this comprehensive base is the system of critical infrastructure that could provide the framework for civilian capability development. Development of civilian capabilities through critical infrastructure should be planned in a prospective approach using a medium to long-term planning horizon. We envisage the possibility to use defence planning system in an integrated manner that could provide the necessary military and civilian capabilities in parallel based on coordinated priorities. It could ensure better possibilities to meet the requirements of countering complex challenges.

BIBLIOGRAPHY:

Besenyő, János, Attila Gulyás and Darko Trifunovic. 2023. Hezbollah and the Internet in the Twenty-First Century. International Journal of Intelligence and Counterintelligence. Volume 36/3. https://doi.org/10.1080/08850607.2022.2111999

Bitzinger, Richard A. 1989. Assessing the Conventional Balance in Europe, 1945-1975. The Rand Corporation, Santa Monica, CA 90406-2138.

Brown, Katherine E. 2022. Transnational Terrorism. In, McGlinchey, Stephen. Foundations of International Relations. London: Bloomsbury, ISSN 2053-8626.

Buzan, Barry, Ole Waever and Jaap de Wilde. 1997. Security: A new framework for analysis, Lynne Rienners Publishers, ISBN 1555877842.

EU 2020. Strategic Foresight Report
https://commission.europa.eu/strategy-and-poliy/strategic-planning/strategic-foresight/2020-strategic-foresight-report_en

EU 1945-1959. History of the European Union https://european-union.europa.eu/principles-countries-history/history-eu/1945-59_en

Lasconjarias, Guillaume. 2017. Deterrence through Resilience, NATO Defence College, Eisenhower Paper Nr. 7, Rome.

ManageEngin 2021. The Colonial Pipeline ransomware attack: Lessons from cybersecurity teams, Manageengin Blog, PLAM 360

https://blogs.manageengine.com/corporate/manageengine/pam360/2021/06/15/the-colonial-pipeline-ransomware-attack-lessons-for-cybersecurity-teams.html

Britannica. 1961. McNamara, Robert S. https://www.britannica.com/biography/Robert-S-McNamara

National Intelligence Council. 2021. Foreign Threats to the 2020 US Federal Elections

https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Government, HUN. 2021. National Military Strategy of Hungary. Budapest.

https://defence.hu/news/national-military-strategy-of-hungary.html#:~:text=Hungary's%20strategic%20objective%20is%20to,and%20non%2Dmilitary%20threats%20and

Government, HUN. 2020. National Security Strategy of Hungary. Budapest.

https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html#:~:text=Our%20primary%20security%20policy%20interest,in%20a%20constantly%20evolving%20environment.

NATO 2016. Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO-ACT 2017. Strategic Foresight Analysis 2017 Report. Norfolk.

https://www.act.nato.int/wp-content/uploads/2023/05/171004_sfa_2017_report_hr-1.pdf

NATO Defence Planning Process,

https://www.nato.int/cps/en/natohq/topics_49202.htm.

Stojkovic, Dejan and Bjørn Robert Dahl. 2007. Methodology for long term defence planning.

https://issat.dcaf.ch/mkd/download/17291/202850/Long%20Term%20Defence%20Planning.pdf

The NDPP (2016), NATO Defence Planning Process, Brussels,

The North Atlantic Treaty. 1949. Washington D.C. https://www.nato.int/cps/en/natolive/official_texts_17120.htm

Tulkoff, Milton L., Vance C. Gordon, Rachel D. Dubin and Wade P. Hinkle. 2010. Planning, Programming, and Budgeting System (PPBS)/Multi-year Programming" Institute for Defence Analyse, IDA Document D-4057 Log: H 10-000982, Alexandria, USA

UN 1945. Charter of the United Nations and Statute of the International Court of Justice, San Francisco. https://treaties.un.org/doc/publication/ctc/uncharter.pdf

DOI: 10.53477/1842-9904-23-11

SANCTIONS EVASION AND VIRTUAL ASSETS: IMPLICATIONS FOR NATIONAL SECURITY

Bogdan VACUSTA*

2022 was the year marking a significant increase in the use of virtual assets for illicit activities such as sanctions evasion. Most of the entities conducting these activities are linked to Russia, North Korea and Iran, which are subject to international sanctions imposed by the international community.

The paper presents key elements about the use of virtual assets in illicit activities by sanctioned entities and highlights the necessity to increase defence and intelligence resources for better data analysis on this type of entities. Analyzing data about virtual assets transactions requires strong collaboration between public and private organizations, with a focus on an intelligence-led approach, considering the growing links between cybercrime, money laundering, terrorist financing, special operations conducted by adversaries. In order to support this collaboration, it is essential to prioritize the education of decision-makers on the necessity to focus on technical data.

Keywords*: sanctions evasion; virtual assets; sanctioned entities; data analysis; blockchain; intelligence.*

Introduction

The Russian invasion of Ukraine and the subsequent sanctions imposed by the international community raised international awareness on the topic of *sanctions evasion*. Even though apparently there are no obvious indicators to identify a major risk towards national security, a closer look shows data about the use of virtual

**** Bogdan VACUSTA is a certified Blockchain/DLT Manager, by the Technical University of Munich, also a Counter Fraud Manager, accredited by the UK Counter Fraud Professional Accreditation Board, and a PhD Candidate for "Mihai Viteazul" National Intelligence Academy doctoral studies. E-mail: bogdan.vacusta@gmail.com***

assets in cybercrime, money laundering, illegal trade, conducted by entities linked to Russia, North Korea and Iran.

Blockchain is the underlying technology facilitating the transfer of value through virtual assets and has the potential to improve different legacy systems and procedures, mainly due to its transparent, permissiveness and distributed nature. However, virtual assets are only one major practical financial application on how blockchain technology can be deployed on a wider scale in the different sectors of activity. Essentially, transactions involving virtual assets have a pseudo-anonymous nature, contrary to common opinions that these are anonymous. The problem is that de-anonymizing them requires a lot of time and resources, which actually affects public confidence in cases of major incidents. The resources allocated from public money involve decisions across a wide range of decision-makers, who have not fully understood yet the technology, the data required to de-anonymize and the necessity to upgrade skills of existing workforce.

This paper provides examples on how virtual assets are used in illicit activities conducted by entities linked to Russia and their affiliates from North Korea and Iran, highlighting the need to improve intelligence gathering capabilities, data analysis and also the education of decision-makers so that regulation can be effective, based on technical data requirements.

A study published by the US Center for Strategic and International Studies (CSIS) provided details regarding the impact of sanctions evasion: "A current risk in today's trade ecosystem is that countries leverage virtual assets to circumvent US sanctions" (Reinsch, Palazzi, 2022). The study also provided examples on how Russia's affiliates, Iran and North Korea, used virtual assets:

- Iran legalized virtual assets payments to pay for imports;
- North Korea hacked into virtual assets wallets and laundered the stolen funds through financial institutions such as Virtual Assets Service Providers (VASPs);
- the North Korean state-sponsored hacking group Lazarus used obfuscation techniques to disguise the source and launder their approximately equivalent of 1 billion USD in virtual assets, obtained from their cyber-crimes since 2015.

The news agency Reuters published in November 2022 an article about Binance, a major VASP (who also has operations in Romania and a significant market share), on how they allowed Iranian firms trade 8 billion USD, even though there are sanctions in place to cut off Iran from the global financial system (Berwick, Wilson, Zamfir, 2022). Binance denied any wrong-doing, however the transactions have taken place. The question about avoiding such situations to occur again has the answer in the available blockchain analysis tools and the decisions to use these in an intelligence-led approach.

Chainalysis, one of the major private companies conducting blockchain analysis, mentioned in their *2023 Crypto Crime Report* that the share of all virtual

assets activity that are linked to illicit activity increased for the first time since 2019, from 0.12% in 2021 to 0.24% in 2022 (Figure no. 1). Overall, illicit transaction volume rose in 2022 for the second consecutive year, hitting an all-time high of 20.1 billion USD (Chainalysis, 2023).

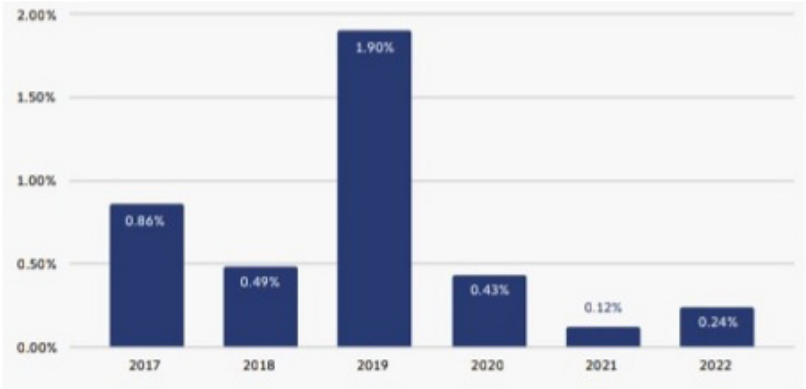

Figure no. 1: Illicit share of all cryptocurrency trading volume (Chainalysis 2023)

The report from Chainalysis mentioned that 44% of the overall illicit 20.1 billion USD came from "activity associated with sanctioned entities" (Figure no. 2), raising by a staggering figure of 10,012,224.34% from 2021 to 2022. The remaining 56% was related to stolen funds, ransomware, fraud, terrorism financing, and other illicit activities.

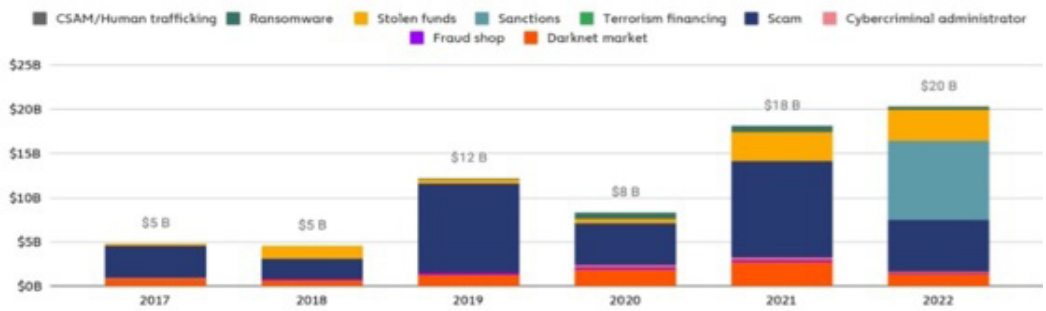

Figure no. 2: Total cryptocurrency value received by illicit addresses (Chainalysis 2023)

In order to assess the impact of sanctions evasion on a specific country level, further blockchain analysis data could be provided by companies such as Chainalysis, but these include proprietary data sets and methodologies which are subject to privacy and confidentiality requirements, this is why this paper only makes reference to data already in the public eye.

It is essential to underline that these are only estimates of illicit virtual assets activity, considering the transparency of most blockchain transactions and allow us to understand why sanctions evasion is becoming a major topic from professionals in finance, law enforcement, defence and intelligence agencies. In order to tackle the risks, improve the accuracy of data (so that we can work not only with estimates) and de-anonymize the illicit transactions, the work between the public sector and the private sector has become essential when it comes to virtual assets.

Companies from the private sector conducting blockchain analysis, such as Chainalysis, Elliptic, TRM Labs etc., can help initially by evaluating the risk of entities involved in virtual assets transactions, but they are not able to complete the cycle and fully de-anonymize the transactions and link specifically virtual assets addresses to individuals because that would imply intrusion into private lives. Only the organizations from the public sector such as defence and intelligence agencies, law enforcement, prosecution bodies can complete the cycle of de-anonymization when illicit activity is identified, by further exploring data sets and risk evaluations obtained from these blockchain analysis companies, cross-referencing these with internal data sets and conducting further intelligence gathering using special methods on risky entities, according to legal frameworks.

1. How Sanctions Evasion Can Be Enforced

The US Treasury's Office of Foreign Assets Control (OFAC) and similar agencies in other jurisdictions (G7, European Union, UK Treasury, Japan Ministry of Economy, Australia Department of Foreign Affairs etc.) implement sanctions through the targeting of individuals, groups, countries, considered threats to national or international security.

"The growing prevalence of virtual assets as a payment method… brings greater exposure to sanctions risk – such as the risk that a sanctioned person or a person in a jurisdiction subject to sanctions might be involved in a virtual currency transaction" warns OFAC in its *Sanctions compliance guidance for the virtual currency industry (*Office of Foreign Assets Control, 2023*)*. For example, in May 2017, North-Korean hackers known as the Lazarus Group, launched the WannaCry ransomware attack, which had damaging effect on individuals, businesses and other organizations, but allowed to generate funds for North Korea's government by requesting payments in virtual assets (US Treasury, 2019). This marked a link between cyber-crime and virtual assets, justifying OFAC to sanction the Lazarus Group by prohibiting US persons from making or facilitating payments to the group.

Traditionally, sanctions enforcement relied on the cooperation of mainstream financial institutions. With virtual assets at the intersection of cybercrime, finance and banking, technology, money laundering and financial crime enforcement, the

role of defence and intelligence agencies is becoming more and more critical to properly assess the problem by gathering intelligence using specific methods. The main challenge now is that the enforcement of sanctions evasion can be conducted by organizations like OFAC only if the approach is intelligence-led. Having reliable data also from international partners of the USA, which could be analyzed properly without waiting for a problem to have systemic implications, is essential. This can be achieved mainly by improving cooperation among authorities, public sector and it requires first a clear understanding of the problem and how it affects current roles, responsibilities and partnerships.

1.1. A closer look on illicit activity

Data obtained from blockchain analysis companies allows to understand better the flow of illicit transactions, decide accordingly where resources should be allocated with priority and what should be the role of public sector organizations in order to achieve de-anonymization of transactions involving entities linked to illicit activity, such as sanctions evasion.

According to Chainalysis crime report, there are different entities used in various combinations by criminals who are processing illicit virtual assets transactions, the biggest volumes in recent years involving two types of entities: Centralized VASPs and Decentralised Finance (DeFi) protocols (Chainalysis, 2023).

Centralized VASPs, mostly controlled by legal entities, were the biggest recipient of illicit virtual assets, because this is the easiest way to convert virtual assets into cash. It may be surprising because internal transactions of a VASP are not available publicly available (theoretically facilitating obfuscation) and most of these VASPs are regulated, with compliance measures in place to report illicit activity to financial intelligence units once detected, but this is what data shows. However, it is important to note that transaction data can be further obtained from most of the regulated VASPs by law enforcement, defence and intelligence agencies, using legal framework, once illegal activity has been detected.

In May 2023, OFAC imposed sanctions on Huriya Private, a company based in the United Arab Emirates. According to the US Department of the Treasury: "Since Russia's full-scale invasion of Ukraine in 2022, Huriya began working quickly to move Russian assets into structures protecting them from sanctions. Huriya also helped high-net-worth Russian Federation nationals procure non-Russian passports under assumed names to avoid financial scrutiny and sanctions." (Office of Foreign Assets Control, 2023)

The governments of Iran and Russia have reportedly been working on a gold-backed virtual asset to be utilized for cross-border payments, which could be an attempt by the two governments to avoid the impact of international sanctions.

Iranian and Russian VASPs also have significant transactions, which requires close monitoring by the defence and intelligence agencies to assess transaction flows involving illicit counterparties or operations. (Kuznetsov, 2023)

As example, TRM Labs, a blockchain analysis company, conducted research on Iran's virtual assets transactions and their findings show sanctioned entities sent less than 2 million USD to Iranian VASPs in 2022 and that Iranians are using Virtual Private Networks (VPNs) to obfuscate their location and fake identity documents (IDs) to bypass the compliance systems of international VASPs (TRM Labs Insights. 2023). In January 2023, Iran's government launched_the National Task Force on Virtual Assets (Financial Tribune, 2023), which should enhance coordination between government institutions on virtual assets-related matters, with meetings of the members taking place twice a month (Central Bank of Iran, intelligence agencies, energy, industry, mining and trade).

A critical element, relevant for data analysis, is the increasing use of DeFi protocols in illicit activities (Figure no. 3), which are technical programs running independently, without obvious link to regulated legal entities.

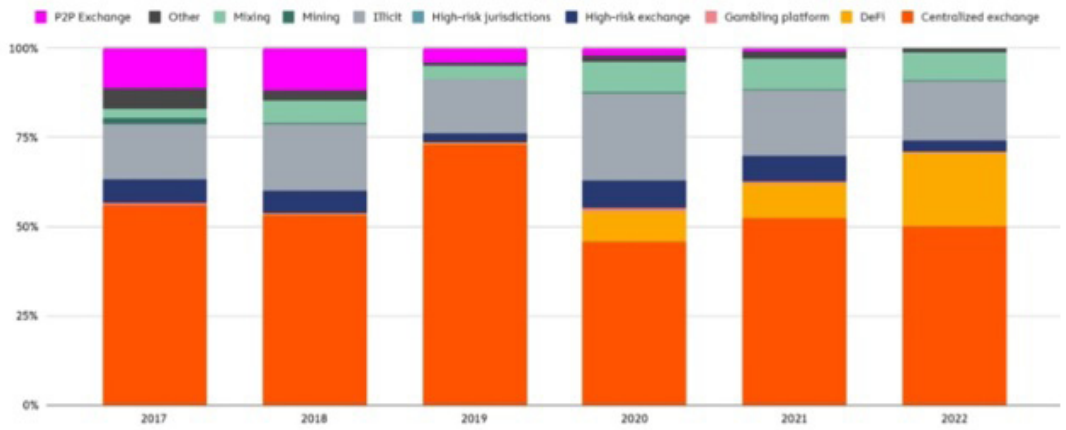

Figure no. 3: Destination of funds leaving illicit wallets
(Chainalysis 2023)

The increasing use of DeFi for illicit activities and not having DeFi regulated under the recently published Markets in Crypto-Assets Regulation in the European Union (Quarta, 2022), leaves a huge data gap when it comes to data analysis involving virtual assets used for illicit activities such as sanctions evasion. In practical terms, law enforcement, intelligence agencies can no longer submit to DeFi protocols a formal request for information as they can do with centralized VASPs, therefore requiring a new methodology for intelligence gathering, data analysis and risk assessments.

All activity involving DeFi is recorded on-chain (unlike centralized VASPs) and DeFi protocols don't allow for the conversion of virtual assets into cash, which in theory may not help criminals to obscure the flow of funds and rapidly monetize their proceeds of crime. But the benefits for criminals with the increasing use of DeFi have to do with cutting the flow of illicit funds (by conducting multiple conversions across different virtual assets, mixers or tumblers and other programmable applications), complicating investigations and delaying legal procedures, which may ultimately affect public confidence and even impact financial stability.

North Korea-linked hackers such as Lazarus Group have deployed multiple hacks over the last few years, in 2022 they stole approx. 1.7 billion USD worth of virtual assets (Figure no. 4). To put this into context, the total value of North Korea's goods exports in 2020 was 142 million USD (The Observatory of Economic Complexity, 2022), this is why many professionals mention that the North Korean government is using the cash obtained from the conversion of stolen virtual assets to fund its nuclear weapons programs (Jin Kang, 2022).

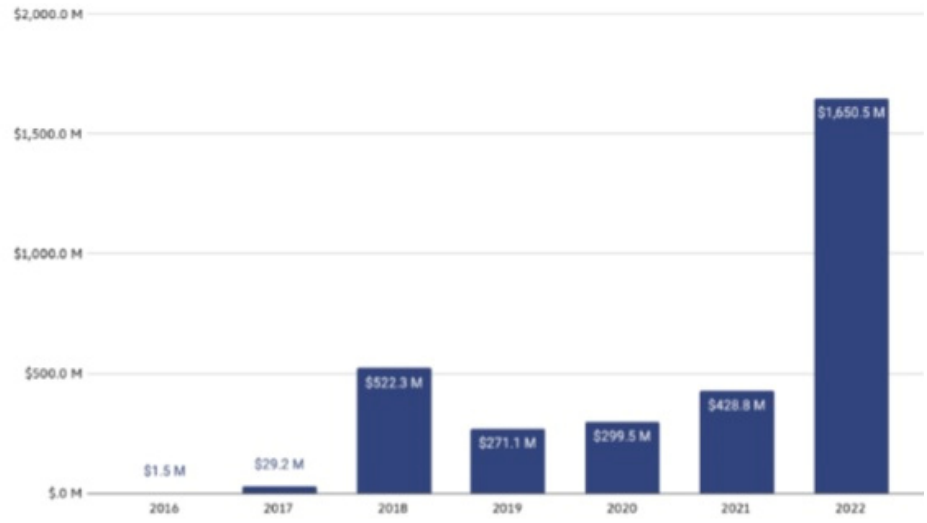

Figure no. 4: Yearly total cryptocurrency stolen by North Korea-linked hackers (Chainalysis 2023)

The Chainalysis report also underlines that 1.1 billion USD of the total 1.7 billion USD, was stolen in hacks of DeFi protocols. After stealing the virtual assets, the North Korea-linked hackers usually sent these assets to other DeFi protocols, mainly because DeFi hacks often resulted in obtaining illiquid virtual assets that aren't listed at centralized VASPs. What hackers usually did by the use of DeFi was to convert those illiquid assets into other virtual assets which have better liquidity. Hackers also sent large sums to mixers, which allow to cut the transaction flow and the origin of funds.

Overall, data from Chainalysis shows that over 40% of illicit virtual assets move first to intermediary services such as mixers or DeFi protocols, with most of those funds coming from high-risk virtual assets addresses such as those linked to sanctions evasion, cyber-crime, money laundering, terrorism financing etc. (Chainalysis, 2023). As a consequence, putting more resources into data analysis involving DeFi transactions and the interactions of criminal entities with DeFi protocols seems reasonable, the key is to build an extensible argumentation so that decision-makers can act accordingly.

1.2. Current trend: Going from individual sanctions to protocol-based sanctions requiring more technical data

The first case involving virtual assets sanctions dates from 2018, when OFAC designated two Iranian nationals associated with the SamSam ransomware strain and included their virtual assets addresses on the Specially Designated Nationals and Blocked Persons (SDN) List entries (US Treasury, 2018).

After 2018, only virtual assets addresses which belong to individuals were included on the SDN List as sanctions identifiers (an average of four addresses per designation in 2019 and nine in 2020). However, in 2021 the designations were extended by also including addresses linked to entities, not only to individuals. The digital currency addresses on the SDN List included their unique alphanumeric identifier (up to 256 characters) while also identifying the blockchain / distributed ledger to which the address corresponds (Office of Foreign Assets Control, 2023).

Overall, the average number of addresses per sanctioned entity reached 35 by 2022, with some designations containing more than 100 virtual assets addresses as identifiers. To have a clearer image, this is a short list of the individuals and entities with virtual assets links sanctioned by US Treasury's OFAC in 2022, along with the reason why these were included on the SDN List:

- Lazarus Group - hacking/theft on behalf of North Korean government;
- Ahmad Khatibi Aghada, Amir Hossein Nikaeen Ravari - ransomware;
- Alex Adrianus Martinus Peijnenburg, Matthew Simon Grimm - drug trafficking;
- Hydra Marketplace - darknet market and money laundering;
- Garantex, Blender.io, Tornado Cash - money laundering;
- Task Force Rusich - Russian paramilitary group in Ukraine.

From the above list, there are two entities which require special attention when it comes to data analysis of virtual assets transactions: Blender.io and Tornado Cash. These are mixers, a frequent method to cut the flow of transactions, working by taking in virtual assets from multiple users, mixing it all together, and sending each user an amount equivalent to what they put in. The result is that each user's virtual assets can now only be traced back to the mixer, rather than to its original source, unless special intelligence and blockchain analysis techniques are employed.

International organizations such as the Financial Action Task Force (FATF) and the US Treasury's Financial Crimes Enforcement Network (FinCEN) have warned that the frequent use of mixers is a red flag and requires careful monitoring and reporting (Financial Action Task Force, 2020 and Elliptic, 2022).

Analysis conducted by the Elliptic blockchain analysis company indicates that North Korea's Lazarus Group laundered virtual assets worth more than 20.5 million USD through Blender.io following the hack of the Ronin Bridge (DeFi service), which resulted in more than 540 million USD of virtual assets as proceeds of crime (Elliptic, 2022). However, sanctioning Blender.io and Tornado Cash did not stop North Korea from progressing further money laundering for their proceeds of crime, but it forced these state-sponsored hackers to find and use alternative mixers, in order to circumvent the sanctions.

Research from Elliptic also indicates that in January 2023, the Lazarus Group sent approximately 58 million USD through another privacy-enhancing service known as Railgun (Elliptic, 2023), which Elliptic had previously identified as an alternative to Tornado Cash (Elliptic, 2022). Elliptic also identified that the Lazarus Group sent virtual assets of more than 100 million USD using another mixer, Sinbad, a DeFi service that was established in October 2022 which appeared to be acting as a replacement for Blender.io following the OFAC sanctions (Elliptic, 2023).

In January 2023, FinCEN designated Bizlatzo, a VASP registered in Hong Kong (under the control of Russians and operating worldwide), as a primary money laundering concern, for failing to "effectively implement policies and procedures designed to combat money laundering and illicit finance" pursuant to Combating Russian Money Laundering Act (Financial Crimes Enforcement Network, 2023). Later, The U.S. Justice Department charged Bitzlato with money laundering (US Attorney's Office, 2023), and competent authorities from Europe reported having seized control of virtual assets wallets containing more than 19 million USD in virtual assets, as part of enforcement actions against Bitzlato (Europol, 2023).

Bitzlato allowed its users to process transactions without minimal identification, becoming a preferred method for using criminal proceeds and funds intended for use in criminal activity. According to US Attorney's Office, Bitzlato's largest counterparty in cryptocurrency transactions was Hydra Market, an anonymous, illicit online marketplace for narcotics, stolen financial information, fraudulent identification documents, and money laundering services that was the largest and longest running darknet market in the world. Hydra Market users exchanged more than $700 million in cryptocurrency with Bitzlato, also received more than $15 million in ransomware proceeds (US Attorney's Office. 2023).

In February 2023, OFAC also undertook a coordinated, joint action alongside the UK's Office of Financial Sanctions Implementation (OFSI) to target ransomware perpetrators (National Crime Agency, 2023). OFAC and the OFSI both sanctioned

seven Russian nationals associated with multiple cyber-attacks. It is important to note that neither OFAC nor OFSI did not include virtual assets addresses belonging to the individuals on their sanctions lists, but the blockchain analysis tool from Elliptic, a private company, identified 53 addresses belonging to six of the seven sanctioned cybercriminals (Elliptic, 2023).

It is the best course of action to avoid designations of individuals on the sanctions list without technical data such as the February 2023's OFAC and OFSI joint action focused on Russians involved in cyber-attacks, which had limited impact on an operational level because virtual assets addresses were not included. In that specific case, the inclusion of the addresses on the list would have had a positive impact by allowing financial institutions to track & monitor those addresses in an effective manner and reporting to competent authorities any counterparty sanctions exposure, mixers or IPs involved, transaction hashes etc.

These examples show the topic of sanctions comes at the intersection of multiple illicit activities and present an obvious obstacle: identifying virtual assets addresses and gathering data linked to transactions of these addresses with other entities in the DeFi space, where there are no centralized entities, which could be approached by law enforcement under legal gateway. Without clearly mentioning the virtual assets addresses, the efficiency of any investigation will be severely impacted.

1.3. Intelligence gathering focused on cross-referencing multiple data sets (geolocation, counterparties receiving / sending funds, mixers etc.)

On 15th of October 2021, OFAC published the "Sanctions Compliance Guidance for the Virtual Currency Industry," which provides best practices to combat the use of virtual assets by sanctioned persons or jurisdictions and highlights its application for VASPs the same as it is done for traditional financial institutions (Office of Foreign Assets Control, 2021). The guidance underlines the use of geolocation tools to prevent IP addresses from sanctioned countries (by using data from multiple sources - IP addresses, Wi-Fi triangulation, GPS signals) and the requirement to implement blockchain analysis monitoring and reporting tools which can identify transactions involving virtual assets addresses associated with sanctioned individuals and entities listed on the Specially Designated Nationals (SDN) list.

Blockchain analysis tools developed by different companies allow collecting and analyzing on-chain data, based on timeline, hashes (unique identifiers), type of blockchain, wallet addresses, VASP and tracing their links to risky entities involved in illicit activity, based on threat intelligence indicators. This kind of output allows financial institutions, intelligence agencies and regulators to follow the financial flow of virtual assets, almost in real time. The nature of blockchains — transparent, permissionless, distributed - allows each transaction to be verified and logged in

a shared, immutable record, along with the time stamp of the transaction and the addresses involved.

In practical terms, adding a virtual assets address to the OFAC's SDN list is followed shortly by marking that address in the blockchain analysis tools developed by Chainalysis, Elliptic, TRM Labs as being connected to a sanctioned entity. Marking it allows later a financial institution, for example, to quickly identify any transactions involving that address, assess the risk, report it to the financial intelligence units or OFAC if it is suspicious or take any other action according to legal requirements. In addition, intelligence and law enforcement professionals can use a blockchain analysis tool to trace and track the movements of virtual assets (to and from an address associated with a reported suspicious address), to build an investigation based on prior intelligence or on the report initially reported by the financial institution to the financial intelligence units or OFAC.

One major challenge in virtual assets is that there is not a single comprehensive list of all virtual assets addresses controlled by sanctioned entities. Having no single list, there is an ongoing need for information about entities involved in transfer of virtual assets by using blockchain technology. The use of blockchain intelligence can partially capture this type of necessary information. The results can turn just a few virtual assets addresses in an OFAC designation into hundreds or thousands other addresses. In the case of Hydra, the darknet market, OFAC included more than 100 virtual assets addresses as identifiers in its designation. However, data from Chainalysis indicates more than 6 million addresses affiliated with Hydra, which are available for monitoring and data analysis (Coindesk, 2023).

Blockchain analytics companies such as Chainalysis are constantly using new data sets which allow them to map better the risk of entities and the links across blockchains. However, it is possible to have undiscovered entities facilitating illicit transactions because there is not enough information available or multiple services are used, which allow obfuscation of funds or location, to avoid detection.

When a traditional financial institution identifies a sanctions exposure, they can block/reject funds and report to OFAC. The limits have to do with the fact that the transaction details are only available to that financial institution, the correspondent institution involved in the transaction, and the regulators which received the report from the financial institution. The significant difference in virtual assets, compared with traditional finance, is that the transaction data is publicly available for everyone on the blockchain – and this is highly relevant when it comes to risk assessments and regulatory reporting.

Information about transactions involving virtual assets can be obtained from a variety of sources, but the path from data and information to intelligence requires cross-reference across multiple technical data sets. These data sets are currently under the control of different public authorities (defence, national security, intelligence,

finance intelligence units, tax data, cyber security operations) or under the control of the regulated financial institutions. Technical data sets held by public authorities also need to be matched across data held by regulated financial institutions such as VASPs, regarding counterparty exposure of their clients, obtained by screening transactions on a risk-based approach.

Historically, financial institutions have solely focused on performing sanction checks on their customers during the onboarding process. Now, only a limited number of financial institutions currently use blockchain analytics (to screen and identify sanctioned virtual assets addresses) or various geolocation tools to uncover if any customers are in sanctioned jurisdictions (device IDs, IP and GPS location, etc.). By encouraging the use of blockchain analytics to assess counterparty exposure and the use of mixers, financial institutions would be in a position to obtain a significant bigger volume of data about suspicious transactions linked to cybercrime, money laundering, terrorism financing etc.

In order to increase the use of blockchain analytics across financial institutions, law enforcement, and intelligence agencies, it is important that decision-makers understand the benefits of using these tools, but also their limits, considering they can only capture part of the overall transactions if data sets are not cross-referenced between public and private entities.

2. Why it is critical to inform decision-makers based on technical data

Traditionally, intelligence agencies have a responsibility to inform decision-makers and recommend a course of action once emerging threats or risks become apparent. In order to have the best course of action to manage the threats or risks involving the use of virtual assets, it is useful to ensure that the intelligence provided to decision-makers also includes minimal technical data which is specifically linked to blockchain technology.

The transfer of value across blockchains is already affecting current working practices and the risks associated with virtual assets in areas such as sanctions evasion cannot be ignored. The sooner more actions are implemented to increase internal capabilities, the better the outcome in terms of data analysis and managing the risks.

Many decision-makers actively participate in national or international working groups linked to cyber-crime, money laundering, terrorism financing, whose work end up often in policies and regulatory frameworks. Such frameworks should include the necessity to focus on data analysis and common reporting mechanisms as the key to achieve a coordinated approach. A recent report published in May 2023 by the European Systemic Risk Board highlighted there is limited information available to assess the exposures and impact of virtual assets, recommending as a policy option to improve processes on how data is assessed, monitored, reported,

also encouraging to work on standardized templates across competent authorities and financial institutions (European Systemic Risk Board, 2023).

Educating decision-makers on blockchain would allow them to understand why it is crucial to focus on tehnical data for a practical outcome, by including technical data in:

- the Early Warning Systems (EWS) linked to red flags on cyber-crime, money laundering, fraud etc.;
- the national risk assessments;
- new specific legislation drafted or updated;
- the global sanctions list (OFAC SDN List; UN Security Council and EU Consolidated List; the UK HM Treasury Consolidated Sanctions List; the Japan Ministry of Economy, Trade and Industry Sanctions List; the Consolidated Canadian Autonomous Sanctions List; the Australia Department of Foreign Affairs and Trade Sanctions List).

Once the technical details are included in the above, regulated financial institutions can proceed accordingly, adapting their internal monitoring systems to capture transactions linked to sanctions evasion while also identifying more easily the entities or individuals involved in operations which may affect the national security. Consequently, any suspicious transactions or transfer of value involving virtual assets can easily be reported to the competent authority (financial intelligence units, cyber-security agencies etc.).

In many instances, a financial institution may have exposure to sanctions evasion that is not easy to identify, by processing transactions for VASPs and their customers that apparently do not have any obvious connection to virtual assets. Without the right tools such as blockchain analytics and sufficient controls in place to detect this type of activity, the financial institution could face significant exposure to virtual assets-related risks.

Managing the risks to the national security arising from the use of virtual assets in illicit actions requires the education of decision-makers, providing them with practical elements so that these can end-up in formal policies, procedures and regulations, which allow financial institutions to have legitimacy in capturing later the useful information for law enforcement, intelligence or defence agencies.

Conclusions

Sanctions evasion involving the use of virtual assets has become a problem affecting national security after the Russian invasion in Ukraine and especially because of the data gap concerning the risks coming from jurisdictions such as Russia, North Korea, Iran, which are involved in illicit activities to support their foreign policy. Covering the data gap requires the use of blockchain analysis data sets

provided by private companies and cross-referencing these with data sets which are under control of public authorities, while also using special defence and intelligence methods to de-anonymize illicit transactions.

A coordinated approach on a national and international level requires the support of decision-makers who need to understand the type of technical data required for analysis, in order to support effective policies, regulations and procedures. Having effectiveness in decisions aimed to tackle the use of virtual assets for sanctions evasion or other illicit activities would also allow defence and intelligence agencies to utilize blockchain technology aimed at compromising their enemies' ability to do so.

In order to ensure coordination and effectiveness of data analysis, it is essential for competent authorities to prioritise setting up a holistic data analysis platform regarding the use of virtual assets for illicit purposes, using consistent and relevant technical criteria, maximising results by using encryption, while also ensuring consistency of relevant data sets.

The national data analysis platform should be managed by a designated competent authority and would require updating the legal framework, having the objective to identify suspicious activity, monitor risky transactions, safeguard national security and financial stability.

Capacity building in blockchain analytics is essential and efforts should be made by all competent authorities to foster the development of relevant expertise and create a community of professionals in this field.

A national data analysis platform built through capacity building would also allow a pro-active approach being implemented, allowing to assess better the interactions between traditional finance and virtual assets, the risks towards financial stability, while also marking transactions used for illegal activities which will be there forever — no public or private entity could erase them from the blockchain.

BIBLIOGRAPHY:

Berwick, Angus & Wilson, Tom. 2022. *"Crypto exchange Bincance helped Iranian firms trade $8 billion despite sanctions"*, Reuters. November 7, 2022. Accessed June 3, 2023. https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04

Chainalysis. *"2023 crypto crime trends"*. January 12, 2023. Accessed May 26, 2023. https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction

Coindesk. 2023. *"Darknet revenues fall after Hydra's shutdown: Chainalysis"*. February 9, 2023. Accessed June 1, 2023. https://markets.businessinsider.com/news/currencies/darknet-revenues-fell-after-hydras-shutdown-chainalysis-1032083033

Elliptic. 2022. *"Examining the FinCEN's crypto asset red flags"*. March 14, 2022. Accessed May 18, 2023. https://www.elliptic.co/blog/examining-the-fincens-

cryptasset-fincen-red-flags?__hstc=267712218.8d1967e3515191c1013500ac7e18de8e.1663668682938.1678455236447.1678790367630.51&__hssc=267712218.1.1678790367630&__hsfp=1520624391

Elliptic. 2022. *"North Korea's Lazarus group identified as explorers behind 4540 million Ronin Bridge theft"*. April 14, 2022. Accessed May 28, 2023. https://hub.elliptic.co/analysis/north-korea-s-lazarus-group-identified-as-exploiters-behind-540-million-ronin-bridge-theft.

Elliptic. 2022. *"Tornado Cash alternatives Briefing note"*. Accessed June 2, 2023. https://hub.elliptic.co/reports/tornado-cash-alternatives-briefing-note

Elliptic. 2023. *"Crypto Mixers and Privacy Protocols: the Sanctions Compliance Implications"*. January 3, 2023. Accessed June 5, 2023. https://hub.elliptic.co/analysis/crypto-mixers-and-privacy-protocols-the-sanctions-compliance-implications/

Elliptic. 2023. *"Has a sanctioned Bitcoin mixer been resurrected to aid North Korea's Lazarus group?"*. February 13, 2023. Accessed May 26, 2023. https://hub.elliptic.co/analysis/has-a-sanctioned-bitcoin-mixer-been-resurrected-to-aid-north-korea-s-lazarus-group

Elliptic. 2023. *"Ransomware and sactions. Using holistic screening to ensure compliance"*. March 21, 2023. Accessed May 12, 2023. https://hub.elliptic.co/analysis/ransomware-and-sanctions-using-holistic-screening-to-ensure-compliance/

European Systemic Risk Board. 2023. *"Crypto-assets and descentralised finance. Systemic implications and policy options"*. Accessed May 28, 2023. https://www.esrb.europa.eu/news/pr/date/2023/html/esrb.pr230525~c74fa66621.en.html

Europol. 2023. Press release*: "Bitzlato: senior management arrested"*. January 23, 2023. Accessed June 8, 2023. https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

Financial Action Task Force. 2020. *"Virtual assets. Red flags indicators of money laundering and terrorist financing"*. Accessed April 27, 2023. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Financial Crimes Enforcement Network. 2023. Press release: *"FinCEN identifies virtual currency exchange Bitzlato as a prime money laundering concern in connection with Russian illicit finance"*. January 18, 2023. Accessed June 8, 2023. https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering

Financial Tribune. 2023. *"Iran Gov't forms crypto task force"*. January 16, 2023. Accessed June 4, 2023. https://financialtribune.com/articles/business-and-markets/116878/iran-gov-t-forms-crypto-taskforce

Jin Kang, James. 2022. *"North Korea's nuclear program is funded by stolen cryptocurrency"*. November 30, 2022. Accessed June 4, 2023. https://theconversation.com/north-koreas-nuclear-program-is-funded-by-stolen-cryptocurrency-could-it-collapse-now-that-ftx-has-195559

Kuznetsov, Mikhail. 2023. *"Russia and Iran began working on a common stablecoin on gold"*. January 16, 2023. Accessed June 4, 2023. https://www.vedomosti.ru/economics/articles/2023/01/16/959100-rossiya-i-iran-nachali-prorabotku-obschego-steiblkoina

National Crime Agency. 2023. Press release*: "Ransomware criminals sanctioned in joint US/UK crackdown on internation cyber crime"*. February 9, 2023. Accessed May 20, 2023. https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime

Office of Foreign Assets Control. 2023. *"Publication of sanctions compliance guidance for the virtual currency industry and updated faqs"*. October 15, 2021. Accessed May 27, 2023. https://ofac.treasury.gov/recent-actions/20211015

Office of Foreign Assets Control. 2023. *"Questions on virtual currency"*. Accessed June 14, 2023. Accessed May 27, 2023. https://ofac.treasury.gov/faqs/topic/1626

Office of Foreign Assets Control. 2023. *"Russia-related Designations"*. May 19, 2023. Accessed May 27, 2023. https://ofac.treasury.gov/recent-actions/20230519

Quarta, Luciano. 2022. *"DeFi and MiCA: another missed opportunity"*. October 13, 2022. Accessed May 27, 2023. https://en.cryptonomist.ch/2022/10/13/defi-mica-another-missed-opportunity

Reinsch, William Alan & Palazzi, Andrea L. 2022. "*Cryptocurrencies and U.S. Sanctions Evasion: Implication for Russia*". December 22, 2022. Accessed May 8, 2023. https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia

The Observatory of Economic Complexity. 2022. *"North Korea – country overview"*. Accessed June 4, 2023. https://oec.world/en/profile/country/prk

TRM Labs Insights. 2023. *"Iran's crypto economy"*. April 17, 2023. Accessed June 4, 2023. https://www.trmlabs.com/post/iran-crypto-economy

US Attorney's Office. 2023. Press release: *"Founder and majority owner of Bitzlato, a cryptocurrency exchange, charged with unlicensed money transmitting"*. January 18, 2023. Accessed June 8, 2023. https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money

US Treasury. 2018. Press release*: "Treasury designated Iran-based financial facilitators of malicious cyber activity and for the first time identifies associated digital currency addresses"*. November 28, 2018. Accessed June 4, 2023. https://home.treasury.gov/news/press-releases/sm556

US Treasury. 2019. Press release: *"Treasury sanctions North-Korean state-sponsored malicious cyber groups"*. September 13, 2019. Accessed June 4, 2023. https://home.treasury.gov/news/press-releases/sm774

Zamfir, Claudiu. 2022. *"Șeful Binance a venit la București: România e o piață importantă"*. September 19, 2022. Accessed March 12, 2023. https://www.startupcafe.ro/afaceri/seful-binance-bucuresti-romania-piata-importanta.htm

DOI: 10.53477/1842-9904-23-12

SOFT COMPUTING IN PREVENTING RANSOMWARE RELYING ON LARGER-SCALE DATA AND ANALYSIS

Attila Mate KOVACS*

Ransomware attacks continue to pose a significant threat to organizations and individuals worldwide. The attackers' ability to constantly evolve and adapt their tactics challenges traditional cybersecurity approaches to keep pace. Ransomware attacks targeting the healthcare industry accounted for 45% of all reported cyberattacks. The nature and scale of attacks and the increasing healthcare technology adoption will continue to pose ransomware attack risks. However, by collecting and analyzing large volumes of data and applying soft computing techniques, cybersecurity experts can improve their ability to detect and prevent ransomware attacks. As a result, soft computing offers options for detecting and preventing malware attacks. Using methods from the field of soft computing, such as fuzzy logic, neural networks, and genetic algorithms, makes it possible to conduct a thorough analysis of large data sets. These can yield insightful information that can help recognize and react to ransomware attacks. These techniques can also help to decrypt files that have been encrypted using ransomware.

Keywords: *soft computing; cybersecurity; ransomware; healthcare; detection; fuzzy logic; genetic algorithm; neural network.*

Introduction

In the last few years, we have witnessed increased concerns from the media, governments, and private sector players regarding the potential damage attributed to cyberattacks. Cyberattacks have continued to develop, taking different forms,

**** Attila Mate KOVACS is a PhD Candidate within Óbuda University Doctoral School on Safety and Security Sciences, Budapest, Hungary. E-mail: attilamate.kovacs@gmail.com***

such as installing spyware in personal computers, spreading worms or viruses, and attempting to destroy a country's critical infrastructures (Christiansen and Piekarz 2019). Computers and other digital devices worldwide are now more susceptible to attacks from different malware. Some of the most common attacks include denial-of-service (DOS), Trojan horses, viruses, worms, blended threats, backdoors, rootkits, email bombs, zombies, and ransomware.

However, ransomware has been the most prevalent malware in the healthcare industry over the past years. Ransomware holds the target data "hostage" for some ransom (Mookherjee et al. 2020). The main focus of ransomware attacks is data availability. Due to the significant impacts of ransomware, recent studies have focused on its growing intensity and threats. Projections now indicate that costs attributed to ransomware attacks will hit over $11.5 billion annually (Hassan 2019). Ransomware attacks will continue to grow up to 350% annually, making the attacks a significant source of threats to critical infrastructures such as healthcare systems. In response, the focus is shifting to the potential use of soft computing to fight ransomware attacks.

For the last three decades, the subject of soft computing has been the focus of substantial scientific investigation. As a result, various soft computing models have found applications in diverse fields, such as agriculture, biological engineering, and information security systems (Mishra, Satapathy, and Chatterjee 2022, 2). The diversity of soft computing models makes soft computing techniques a reliable strategy for solving complex problems. Significantly, over the last few decades, there has been a constant increase in the usage of soft computing to combat cyberattacks in the field of information security. The paper reviews the literature on large-scale ransomware attacks and the use of soft computing in the fight against cyberattacks.

Methodology

The paper adopts a qualitative case study approach to review, synthesize, and make study recommendations. Qualitative research methodology focuses on understanding a humanistic query as an idealistic approach (Pathak, Kalra, and Jena 2013). The authors reiterate that the qualitative method is reliable due to its basis on numeric and strategies that other researchers can use and propagate objectively. Conversely, the qualitative case study technique investigates and analyses single or collective cases to reflect the intricate nature of the research target (Hyett, Kenny, and Dickson-Swift 2014, 2). In this respect, a case is an object under study based on a particular or peculiar reason. In addition, the classification and selection of cases help to clarify the study topic and design the study strategy. As a result, there are three study cases and study design frameworks. The case study frameworks are the intrinsic case, the instrumental case, and the collective instrumental case (Rubin and Babbie. 2016).

The objective of the intrinsic case, as opposed to understanding the function of a case, is to gain insight into the particulars of a single item. (Hyett, Kenny, and Dickson-Swift 2014, 2). An instrumental case is employed to elucidate an issue under study or refine a particular theory. Such a case study is adopted to promote a better comprehension of an object of interest. A collective case study, on the other hand, is an instrumental study that makes use of numerous nested cases. This paper adopts a collective qualitative case study focusing on the objects of ransomware and software computing. The qualitative approach was chosen owing to the numerous benefits associated with the methodology. Because the researcher had access to the most recent, high-quality data, qualitative research technique offers a thorough grasp of a studied subject or area (Pathak, Kalra, and Jena 2013, 46).

Hypothesis

The paper is intended to test the following hypothesis: "If soft computing models can imitate human brains, can soft computing help fight against the threats of ransomware"? Besides, the paper hypothesizes that combining vast data samples and soft computing techniques can enhance ransomware detection and prevention. Consequently, the paper collects and assesses large data samples based on ransomware attacks while using soft computing literature to test the hypothesis. When large ransomware data samples and soft computing strategies are combined, the result can enhance overall cybersecurity, leading to effective detection, quicker reaction times, and less downtime.

Moreover, gathering large data samples on ransomware attacks can make it possible to develop more efficient machine-learning models, resulting in increased detection skills. By combining these strategies, businesses can strengthen their defence against ransomware attacks, minimizing the damage caused by successful attacks and reducing future assaults. According to the paper, preventing ransomware attacks will require a combination of the accumulation and analysis of large data samples and the application of soft computing techniques.

Literature Review

Initially, scholars and practitioners believed that ransomware originated in Russia. However, Information Resources Management Association (2021) outlines the explosion of cyberattacks in the past 12 years that demystified the myth (see Figure no. 1 for timeline). A review of historical cases of attacks proved that ransomware existed in other parts of the world, including North America and Asia.

Besenyő et al. (2021, 2-3, 24) has analyzed terrorism targeting healthcare facilities and workers since the 9/11 attacks. Their study highlights the vulnerability

of healthcare systems to various threats. This research underscores the importance of enhancing security measures within the healthcare sector, including detecting and preventing attacks. By examining the multiple challenges healthcare facilities face in dealing with terrorism and other threats, this study provides valuable context for understanding the broader implications of attacks and the need for effective countermeasures.

The history of malware can date back to 1970s, when the first malicious programs gained popularity in entertainment (Abaimov and Martellini 2022). Since then, malware has evolved, with the first ransomware detected in 1989 introduced as "AIDS Trojan". The Trojan tricked PC users leading them to encrypt and hide files on a computer drive, which required the owner to pay some ransom for decrypting the files (Kumar et al. 2021, 380). The explosion of the attacks remains the subject of great scrutiny in cybercrime. Research indicates that if unchecked, ransomware will implode and reach levels that could create devastating impacts. As a result, there has been increasing interest in and use of various soft computing techniques (Dawn et al. 2020, 924).

Figure no. 1: The Ransomware Timeline
(Source: Information Resources Management Association 2021)

Researchers believe that traditional methods in the fight against ransomware must be improved (Information Resources Management Association 2021, 1087) to better understand its impacts and advance better prevention and control strategies.

To situate ransomware in the context of malware, it can also be described as a fundamental explanation that ransomware is a malicious malware that conceals files on a target computer or network and demands payment for the decryption key required to release the contents (Abaimov and Martellini 2022). The attackers typically require payment in a cryptocurrency such as Bitcoin, making it difficult to trace the money and the attackers themselves. Ransomware has increased in the scale of attacks, affecting different countries and sectors (see Appendix 1).

Researchers classify ransomware attacks into several categories. According to Fields (2018), ransomware attacks comprise five main categories based on target platforms. Ransomware can take different forms and infect either a personal computer, mobile device, cloud storage, servers, and smart TV sets (Hassan 2019). Regardless of the ransomware category, the authors note that its attacks continue to produce adverse consequences for individuals and organizations. However, ransomware attacks on organizations are typically large-scale and specialized in targeting specific organizations to achieve certain goals.

There are various ways in which ransomware attacks can take place. Fields (2018) states that ransomware attacks can occur through email attachments, malicious links, and software vulnerabilities. In addition, some ransomware appears in lock screen attacks, such as CovidLock, which rely on the user's input to execute a code (Modlin, Amber and Gregory, Andrew and Odebode, Iyanuoluwa and Hodson, Douglas and Grimaila, Michael. 2021, 33). After the virus installs on a device, it typically begins encrypting data and presenting a message to the user demanding money in return for the decryption key (Kovács 2022, 98, 100). Once this process is complete, the malware will typically remove itself.

1. Incidences of Ransomware Attacks

Review cyberattacks indicate that ransomware attacks remain challenging for many organizations and sectors. Alqahtani and Sheldon (2022) note that ransomware attacks affect critical cyber-physical systems and continue to attack many users. In an empirical study involving 50 organizations in the UK and North America, Yuryna Connolly et al. (2020, 2) found that private sectors have faced severe effects of crypto-ransomware attacks. Also, the authors noted that the organization's size was not a factor in ransomware attacks. Ransomware attacks are becoming increasingly common and are a significant threat to sectors that provide critical services. These sectors include healthcare, finance, energy, transportation, and government agencies. These industries are particularly vulnerable because they handle sensitive data and provide essential services that are crucial to the functioning of society.

The healthcare industry is disproportionately affected by ransomware attacks, despite the fact that they affect all enterprises. In the healthcare sector, ransomware attacks continue to be the most common type of cybercrime that is recorded (Mookherjee et al. 2020, 581). During the course of eight years starting from early 2010, the number of ransomware attacks in the healthcare sector has increased by more than 125 percent (Abraham, Chatterjee, and Sims 2019, 547-48). Ransomware is a malicious malware that conceals files on a target computer or network, while demanding for payment to gain access to a decryption key needed to unlock the files. As the healthcare sector expands and transitions digitally, it becomes more

vulnerable, accounting for at least 45% of all cyberattacks (Thamer and Alubady 2021, 213-215). During the COVID-19 pandemic, the US Department of Health Services reports that at least four states fell victim to ransomware, while another 400 hospitals were reportedly on the target list (Dullea, Budke, and Enko 2020, 534). One of the renowned ransomware attacks targeting numerous healthcare systems is the WannaCry, which affected Britain's National Health Services (NHS) (Fields 2018, 85). The WannaCry attack paralyzed operations in over 80 hospitals for four days, leading to delays in clinical appointments and scheduled surgeries (Tully et al. 2020, 229). The other notable ransomware attacks in the healthcare sector are the 2016 Hollywood Presbyterian Hospital in California, which held the hospital's data hostage for ten days until it paid a ransom of $17,000 in bitcoin (Gagneja 2017,1-5). Hospitals are now the primary target for ransomware attacks due to the increasing storage of patient information in digital systems and security holes in hospital information technology systems (see Appendix 2).

Ransomware attacks in the healthcare industry come in different mechanisms. Table no. 1 indicates that cyberattacks targeting the healthcare industry come in nine forms (Alvarez 2017). Notwithstanding the forms of attacks, the incidences of ransomware targeting hospitals rose in 2015 (Nikki et al. 2018, 1, 21-22). A review of reported cases of ransomware indicates that its impacts spread worldwide, with the US being the most affected country (see Appendix 1). Most ransomware attacks affect developed countries, where digital medical information is more valuable to cybercriminals. Similarly, in developed countries, ransomware attacks affect critical national sectors such as transport, healthcare, government agencies, commercial facilities, and energy (Moallem 2020).

Table no. 1: Common Mechanisms of Attacks in Healthcare

Mechanism of Attack	Frequency of Attack
Injected unexpected items	47%
Manipulate data structures	19%
Manipulate system resources	9%
Employ probabilistic techniques	6%
Indicator	6%
Abuse existing functionality	4%
Collect and analyze information	4%
Engage in deceptive interactions	3%
Subvert access control	2%

Attacks within healthcare severely affect individuals and organizations, causing data loss, financial harm, and reputational damage (Fields 2018; The DoD Cyber Exchange 2020). For instance, in 2016 alone, over 73 million ransomware attacks were detected within the healthcare industry (Slayton 2018, 287-288, 293). Of the reported events, nearly 1,500 attacks occurred, and a record of 300 serious incidences. With projections indicating that ransomware attacks may quadruple by 2023, there is a need for preventive strategies. Maintaining up-to-date software, using strong passwords, and exercising caution while reading emails or clicking on links from unfamiliar sources are crucial to avoid ransomware attacks. It is essential to perform frequent data backups to protect against data loss in case of an attack (Singh and Sittig 2016). Government agencies, cybersecurity institutions such as the Cybersecurity and Infrastructure Security Agency (CISA), and private sector recommends strategies such as planning, joint partnerships, preparation, and information sharing (King 2022). However, the evolution in soft computing might provide a timely strategy to avert the impacts of ransomware attacks.

2. Soft Computing

Slayton (2018, 295) outlines that ransomware attacks stood at over 70 million in 2016. Given that the ransomware attacks could rise to numbers that might be complex to manage, research point to the ineffectiveness of conventional approaches (Information Resources Management Association 2021, 1087). The authors attribute the ineffectiveness of conventional methods to the widening cyberspace and increasing numbers of malware. Effective intelligent systems based on challenges under focus and combining appropriate soft computing techniques can be adapted to solve problems. Soft computing is critical in designing intelligent systems that can predict and help solve threats attributed to complex problems.

Soft computing continues to gain relevance in the fight against ransomware. Ransomware attacks continue to rise worldwide, devastatingly impacting critical infrastructures. However, the advanced artificial intelligence (AI) in soft computing has led to advances that can be employed to solve complex ransomware challenges (Shin and Xu 2017, 1). Soft computing is a subfield of Artificial Intelligence (AI) that focuses on creating intelligent algorithms and methods to cope with uncertainty, imprecision, and partial truth in data. AI in soft computing is gaining application in the fight against malware in computing systems and other digital devices.

Research shows that soft computing applications can be applied to detect and prevent ransomware in Android devices. For example, Zhang et al. (2021) found TC-Droid, an automatic threat detection framework for Android, to be effective in malware detection. Similarly, Grini, Shalaginov, and Franke (2018, 337-338) outline the importance of soft computing in overcoming the complexities of modern

ransomware. This paper outlines the importance of soft computing in addressing the complexities of modern ransomware. It demonstrates the effectiveness of using static features extracted from PE32 files and applying Bayesian networks for large-scale malware detection. Using static features extracted from PE32 to study large-scale malware detection, the authors found Bayes Network compelling. In a comprehensive study by Filiz et al. (2021), the authors tested 78 antimalware tools against a sample of 61 ransomware variants. Their findings revealed that the tested tools had minimal impact in effectively combating these ransomware threats. As a result, the authors recommended the adoption of soft computing techniques as more effective alternatives in dealing with ransomware attacks. This study supports the hypothesis that soft computing can enhance ransomware detection and prevention, offering a more robust approach compared to traditional antimalware tools.

Furthermore, Dutta et al. (2021) consent that the best way to combat malware is to use reverse engineering and machine learning. Mohammad (2020) suggests pursuing artificial intelligence in the fight against ransomware in addition to preventive strategies. Sharma et al. (2019, 323-324, 337-338) acknowledge that the complexity of ransomware threats and the data scale requires suitable countermeasures such as fuzzy logic. Similarly, Dovom et al. (2019,2) note that fuzzy logic and fast fuzzy pattern trees provide robust and powerful malware detection. These studies recommend soft computing techniques such as machine learning and artificial intelligence over traditional strategies. Thus, the future in the fight against ransomware might be the application of soft computing strategies. Understanding soft computing techniques is critical in their application against ransomware threats.

Since ransomware is a computer program, soft computing techniques provide a way of analyzing, detecting, and preventing attacks. Soft computing aims to imitate the human brain's capacity to reason and solve issues while operating in an unpredictable and imprecise environment, unlike conventional computer approaches, which depend on specific rules and deterministic models (Shin and Xu 2017). The following are the three primary components of soft computing:

− Fuzzy logic: a mathematical framework that addresses questions of ambiguity and imprecision in data (Dovom et al. 2019,3). Fuzzy logic makes it possible to represent and manipulate nebulous or ambiguous ideas, such as "warm" or "tall," which are complex to describe using typical binary logic;

− Neural or artificial neural networks: computer systems designed to replicate the structure and function of the human brain (Gupta 2021). The networks can learn from data, spot patterns, and make predictions based on information that may be noisy or inadequate;

− Evolutionary computation: refers to a group of optimization algorithms modeled after the processes that occur during biological evolution (Khoda et al. 2021). These algorithms use several strategies to find optimum solutions in spaces

with large dimensions and complicated structures, such as mutation, crossover, and selection.

Research continues to gain momentum in intrusion detection within computer and network security (Sathesh 2019, 72). Techniques from the realm of soft computing are increasingly finding applications in various domains, including control systems, image processing, data mining, pattern recognition, and decision-making systems (Abbasi et al. 2022). Researchers are now proposing different models to detect and prevent malware in Internet of Things (IoT) devices (Khoda et al. 2021). Soft computing models and theories developed to fight ransomware include fuzzy set theory, novel loss function, and particle swarm optimization. These strategies are incredibly effective when working with real-world situations that are complex to solve using typical computer approaches. Soft computing techniques have several applications in cybersecurity (Shin and Xu 2017). Some of the soft computing applications in cybersecurity are:

− Intrusion detection: soft computing strategies such as fuzzy logic and neural networks facilitate detecting network intrusions by analyzing traffic and identifying suspicious activities (Gupta 2021);

− Malware detection: soft computing techniques such as genetic algorithms help detect new and unknown malware by analyzing the behavior of programs and identifying patterns that indicate malicious activity (Lee, Lee, and Yim 2023, 15);

− Spam filtering: soft computing techniques such as neural networks and fuzzy logic apply in filtering spam emails by analyzing the content and identifying patterns that indicate spam (Ahmed et al. 2022, 4);

− Password cracking: soft computing techniques such as genetic algorithms are critical in cracking passwords by generating and testing many possible passwords until it finds the correct one (Shin and Xu 2017);

− Network security: soft computing techniques continue to find applications in optimizing network security by identifying vulnerabilities and developing strategies for mitigating the risk of attacks (Shin and Xu 2017);

− Overall, soft computing techniques have proven helpful in enhancing cybersecurity by providing practical solutions to cybersecurity challenges.

3. Soft Computing in Ransomware Protection

Techniques that make use of soft computing have the potential to play a key role in strengthening the security of healthcare information technology systems (Tully et al. 2020, 230). Healthcare IT security is critical due to the sensitive nature of patient data, including personal information and medical records. Soft computing can improve healthcare IT and security in more ways than one.

Soft computing plays a critical role in anomaly detection. The principles of soft computing help construct intelligent systems capable of recognizing user behavior

patterns and detecting abnormalities that suggest a ransomware attack (Shin and Xu 2017). Soft computing intelligent systems may assist in preventing the ransomware from carrying out its intended function and encrypting the victim's data. In addition, soft computing help analyze the danger of a ransomware attack and uncover weaknesses in the victim's system (Yuryna, Connolly et al. 2020, 7). Furthermore, soft computing approaches may also help avoid ransomware attacks by identifying malicious software or abnormalities, evaluating risk, and building reaction plans (Yuryna Connolly et al. 2020, 17).

Victims can lower the danger of ransomware attacks and keep their data from being encrypted and held for ransom if they combine these approaches with other cybersecurity measures. Moreover, soft computing plays a significant role in intrusion detection. According to Sharma et al. (2019, 336-337), neural networks and fuzzy logic in soft computing find applications in detecting network intrusions by monitoring network traffic and recognizing patterns that suggest suspicious behavior, which can prevent access to medical records. Risk assessment may aid the victim in developing effective security methods and allocating resources. In case a ransomware attack occurs, response plans, such as backup and recovery plans, incident response plans, and communication plans, may be developed using soft computing approaches. Incident response plans can assist the victim in responding swiftly and efficiently to a ransomware attack, reducing the damage and swift recovery of the impacted systems.

Similarly, soft computing methods are beneficial in analyzing the risk of cyberattacks and finding vulnerabilities in healthcare IT systems. Risk assessment is essential to vulnerability analysis against cybersecurity threats attributed to ransomware. Vulnerability analysis in healthcare is critical in developing successful security measures and the proper allocation of resources. Research also points to the effectiveness of soft computing strategies in malware detection (Dovom et al. 2019, 7). Soft computing methods such as genetic algorithms help discover new and unknown malware by monitoring the behavior of programs and detecting patterns that signal harmful activity. It also aids in behavior monitoring through behavioral analysis. Thus, the latter is critical in the protection of patients' data against malicious software.

Finally, soft computing strategies help develop effective access control. Soft computing techniques improve access control mechanisms by developing intelligent systems that recognize user behavior patterns and detect anomalies that indicate unauthorized access. Access control helps prevent data breaches, ensuring only authorized people can access patient information. In general, the security of healthcare information technology systems might be significantly enhanced with the application of soft computing techniques.

Large Sample Data Collection is Essential in Cybersecurity for Several Reasons:

− Improving accuracy: large sample data collection allows for more accurate analysis and prediction of cybersecurity threats (Aurangzeb et al. 2022). A more extensive data set helps identify patterns and trends that may slip through with a smaller sample size;

− Identifying new threats: large sample data collection can help identify new, emerging, less visible threats (Aurangzeb et al. 2022). By analyzing a large volume of data, cybersecurity experts can detect patterns that indicate the presence of new types of malware or cyberattacks;

− Enhancing machine learning: machine learning algorithms require large data sets to be trained effectively (Aurangzeb et al. 2022). With more data, the algorithms can effectively and accurately detect cybersecurity threats;

− Supporting incident response: large sample data collection can provide valuable insights into how cyberattacks occur and how they can be prevented or mitigated (Aurangzeb et al. 2022). New insights are invaluable in developing incident response plans that are more effective against cyberattacks;

− Enabling threat intelligence sharing: large sample data collection can support sharing threat intelligence information between organizations (Aurangzeb et al. 2022).

Organizations can better prepare and defend against cyberattacks by sharing information on cybersecurity threats. Hence, Aurangzeb et al. (2022) reiterate that extensive sample data collection is essential in cybersecurity. It allows for more accurate analysis, identification of new threats, enhanced machine learning, improved incident response, and better threat intelligence sharing. Thus, cybersecurity experts can stay ahead of evolving threats and protect organizations from cyberattacks.

4. Summary – Potential Application

Soft computing techniques have the potential to contribute to preventing ransomware attacks in the following ways:

− Malware detection: soft computing techniques such as genetic algorithms and neural networks can detect new and unknown malware by analyzing programs behavior and identifying patterns that indicate malicious activity. Detection is critical in preventing ransomware's spread and protecting the victim's data.

− Anomaly detection: soft computing techniques find use in intelligent systems that can recognize user behavior patterns and anomalies that indicate a ransomware attack. Intelligent systems can help prevent ransomware from executing and encrypting the victim's data.

− Risk assessment: soft computing techniques are critical in assessing the risk of a ransomware attack and identifying vulnerabilities in the victim's system. Risk assessment helps in developing effective security strategies and appropriate resource allocation.

− Response planning: soft computing techniques help respond to ransomware attacks through backup and recovery plans, incident response plans, and communication plans. Response plans are critical in minimizing the damage and restoring the affected systems as soon as possible.

Conclusion

There is a growing adoption of technology across all sectors of national economies worldwide. While technology adoption increases workplace efficiency, they are prone to attacks. Cybersecurity has emerged as one of the greatest challenges facing governments and private sectors worldwide. The critical infrastructure such as the healthcare sector, is becoming the main target of cyberthreats such as ransomware attacks owing to the sensitive information in such sectors. Attacks on critical infrastructure can cripple essential services such as healthcare services, water provision, and electricity supply. Such attacks can be catastrophic to the society and may pose a threat to the national security. However, using large data samples, it is now possible to collect data on ransomware attacks and employ soft computing techniques such as fuzzy logic to detect and assess risks, and develop response plans to prevent ransomware attacks and its impacts.

BIBLIOGRAPHY:

Abaimov, Stanislav, and M. Martellini. 2022. *Machine Learning for Cyber Agents: Attack and Defence*. Cham, Switzerland: Springer.

Abbasi, Muhammad Shabbir, Harith Al-Sahaf, Masood Mansoori, and Ian Welch. 2022. "Behavior-Based Ransomware Classification: A Particle Swarm Optimisation Wrapper-Based Approach for Feature Selection."*Applied Soft Computing* 121 (March): 108744. https://doi.org/10.1016/j.asoc.2022.108744.

Abraham, Chon, Dave Chatterjee, and Ronald R. Sims. 2019. "Muddling Through Cybersecurity: Insights from the U.S. Healthcare Industry." *Business Horizons* 62 (4): 539–48. https .

Ahmed, Naeem, Rashid Amin, Hamza Aldabbas, Deepika Koundal, Bader Alouffi, and Tariq Shah. 2022. "Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges." Edited by Wenjia Li. *Security and Communication Networks* 2022 (February): 1–19. https://doi.org/10.1155/2022/1862888.

Alqahtani, Abdullah, and Frederick T. Sheldon. 2022. "A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook." *Sensors* 22 (5): 1837. https://doi.org/10.3390/s22051837.

Alvarez, Michelle. 2017. "Security Trends in the Healthcare Industry: Data Theft and Ransomware Plague Healthcare Organizations." *IBM Security*. Somers, New York: IBM. ibm.com.

Aurangzeb, Sana, Haris Anwar, Muhammad Asif Naeem, and Muhammad Aleem. 2022. "BigRC-EML: Big-Data Based Ransomware Classification Using Ensemble Machine Learning." *Cluster Computing* 25 (March): 3405–22. https://doi.org/10.1007/s10586-022-03569-4.

Besenyő, János, Márton, Krisztina, & Shaffer, Ryan (2021). Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers. Studies in Conflict & Terrorism 2021, Studies in Conflict & Terrorism, 1-24. https://doi.org/10.1080/1057610X.2021.1937821.

Christiansen, Bryan, and Agnieszka Piekarz. 2019. *Global Cyber Security Labor Shortage and International Business Risk*. Hershey, Pennsylvania: IGI Global.

Dawn, Subhojit, Valentina Emilia Balas, Anna Esposito, and Sadhan Gope. 2020. *Intelligent Techniques and Applications in Science and Technology: Proceedings of the First International Conference on Innovations in Modern Science and Technology*. Cham, Switzerland: Springer International Publishing.

Dovom, Ensieh Modiri, Amin Azmoodeh, Ali Dehghantanha, David Ellis Newton, Reza M. Parizi, and Hadis Karimipour. 2019. "Fuzzy Pattern Tree for Edge Malware Detection and Categorization in IoT." *Journal of Systems Architecture* 97 (August): 1–7. https://doi.org/10.1016/j.sysarc.2019.01.017.

Dullea, Erik, Chris Budke, and Pete Enko. 2020. "Cybersecurity Update: Recent Ransomware Attacks against Healthcare Providers." *Missouri Medicine* 117 (6): 533–34. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7721413/.

Dutta, Nitul, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, and Emil Pricop. 2021. "Introduction to Malware Analysis." *Studies in Computational Intelligence*, October, 129–41. https://doi.org/10.1007/978-981-16-6597-4_7.

Fields, Ziska. 2018. *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*. Hershey, Pennsylvania: IGI Global.

Filiz, Burak, Budi Arief, Orcun Cetin, and Julio Hernandez-Castro. 2021. "On the Effectiveness of Ransomware Decryption Tools." *Computers & Security* 111 (December): 102469. https://doi.org/10.1016/j.cose.2021.102469.

Gagneja, Kanwalinderjit K. 2017. "Knowing the Ransomware and Building Defense against It - Specific to Healthcare Institutes." *2017 Third International Conference on Mobile and Secure Services (MobiSecServ)*, February 1–5. https://doi.org/10.1109/MOBISECSERV.2017.7886569

Grini, Lars Strande, Andrii Shalaginov, and Katrin Franke. 2018. "Study of Soft Computing Methods for Large-Scale Multinomial Malware Types and Families Detection." *Recent Developments and the New Direction in Soft-Computing Foundations and Applications*, 337–50. https://doi.org/10.1007/978-3-030-47124-8.

Gupta, Brij B., ed. 2021. *Advances in Malware and Data-Driven Network Security*. IGI Global.

Hackett, Robert, 2016: "How One Health Care Organization Dodged the Ransomware Bullet." Fortune, May 7, 2016. https://fortune.com/2016/05/07/health-care-ransomware/.

Hariri-Ardebili, Mohammad Amin, Fernando Salazar, Farhad Pourkamali-Anaraki, Guido Mazzà, and Juan Mata. 2023. "Soft Computing and Machine Learning in Dam Engineering." *Water* 15 (5): 917. https://doi.org/10.3390/w15050917.

Hassan, Nihad A. 2019. *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*. New York, NY: Apress.

Hyett, Nerida, Amanda Kenny, and Virginia Dickson-Swift. 2014. "Methodology or Method? A Critical Review of Qualitative Case Study Reports." *International Journal of Qualitative Studies on Health and Well-Being* 9 (1): 23606. https://doi.org/10.3402/qhw.v9.23606.

Information Resources Management Association. 2021. *Research Anthology on Artificial Intelligence Applications in Security*. Hershey, Pennsylvania: IGI Global.

Khoda, Mahbub E., Joarder Kamruzzaman, Iqbal Gondal, Tasadduq Imam, and Ashfaqur Rahman. 2021. "Malware Detection in Edge Devices with Fuzzy Oversampling and Dynamic Class Weighting." *Applied Soft Computing* 112 (November): 107783. https://doi.org/10.1016/j.asoc.2021.107783.

King, Steve. 2022. Losing the Cybersecurity War, CRC Press. Kovács, A. M. 2022. "Ransomware: A Comprehensive Study of the Exponentially Increasing Cybersecurity Threat." *Insights into Regional Development* 4 (2): 96–104. https://doi.org/10.9770/IRD.2022.4.2(8).

Kumar, Raghvendra, Nguyen Ho Quang, Vijender Kumar Solanki, Manuel Cardona, and Prasant Kumar Pattnaik. 2021. *Research in Intelligent and Computing in Engineering*. Cham, Switzerland: Springer Nature.

Lee, Kyungroul, Jaehyuk Lee, and Kangbin Yim. 2023. "Classification and Analysis of Malicious Code Detection Techniques Based on the APT Attack." *Applied Sciences* 13 (5): 2023, 13, 2894. https://doi.org/10.3390/app13052894.

Mishra, Debesh, Suchismita Satapathy, and Prasenjit Chatterjee. 2022. *Soft Computing and Optimization Techniques for Sustainable Agriculture*. India: Walter de Gruyter GmbH & Co KG.

Moallem, Abbas. 2020. HCI for Cybersecurity, Privacy and Trust, 1st edn, Springer Nature. Modlin, Amber and Gregory, Andrew and Odebode, Iyanuoluwa and Hodson, Douglas and Grimaila, Michael. (2021). CovidLock Attack Simulation. https://doi.org/10.1007/978-3-030-69984-0_3. In: Arabnia, Hamid R. 2021. *Advances in Parallel and Distributed Processing, and Applications: Advances in Parallel & Distributed Processing, and Applications: Proceedings from PDPTA'20, CSC'20, MSV'20, and GCC'20*. Cham, Switzerland: Springer Nature. 25-34. https://doi.org/10.1007/978-3-030-69984-0

Mohammad, Adel Hamdan. 2020. "Ransomware Evolution, Growth and Recommendation for Detection." *Modern Applied Science* 14 (3): 68–74. https://doi.org/10.5539/mas.v14n3p68.

Mookherjee, Somnath, Lauren A. Beste, Jared W. Klein, and Jennifer Wright. 2020. *Photography in Clinical Medicine*. Cham, Switzerland: Springer.

Nikki, Spence, Bhardwaj Niharika, Paul David, and Coustasse Alberto. 2018. "Ransomware in Healthcare Facilities: A Harbinger of the Future?" *Perspectives in Health Information Management; Chicago*, 1–22.

Pathak, Vibha, Sanjay Kalra, and Bijayini Jena. 2013. "Qualitative Research." *Perspectives in Clinical Research* 4 (3): 192. https://doi.org/10.4103/2229-3485.115389.

Rubin, Allen, and E. R. Babbie. 2016. *Essential Research Methods for Social Work*. 4th ed. Boston, MA: Cengage Learning.

Sathesh, A. 2019. "Enhanced Soft Computing Approaches for Intrusion Detection Schemes in Social Media Networks." *Journal of Soft Computing Paradigm* 2019 (2): 69–79. https://doi.org/10.36548/jscp.2019.2.002.

Sharma, Arushi, Ekta Gandotra, Divya Bansal, and Deepak Gupta. 2019. "Malware Capability Assessment Using Fuzzy Logic." *Cybernetics and Systems* 50 (4): 323–38. https://doi.org/10.1080/01969722.2018.1552906.

Shin, Yung C., and Chengying Xu. 2017. *Intelligent Systems: Modeling, Optimization, and Control*. New York, NY: CRC Press.

Singh, Hardeep and Sittig, Dean. 2016. 'A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks', Applied Clinical Informatics, vol. 07, no. 02, pp. 624–632. Slayton, Thomas B. 2018. "Ransomware: The Virus Attacking the Healthcare Industry." *Journal of Legal Medicine* 38 (2): 287–311. https://doi.org/10.1080/01947648.2018.1473186.

Thamer, Noor, and Raaid Alubady. 2021. "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research." *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, April, 210–16. https://doi.org/10.1109/bicits51482.2021.9509877.

The DoD Cyber Exchange. 2020. "Cybersecurity Awareness Month – DoD Cyber Exchange." Public.cyber.mil. 2020. https://public.cyber.mil/cybersecurity-awareness-month/.

Tully, Jeff, Jordan Selzer, James P. Phillips, Patrick O'Connor, and Christian Dameff. 2020. "Healthcare Challenges in the Era of Cybersecurity." *Health Security* 18 (3): 228–31. https://doi.org/10.1089/hs.2019.0123.

Winton, Richard. 2016. "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating." Los Angeles Times, February 18, 2016. https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Yuryna Connolly, Lena, David S. Wall, Michael Lang, and Bruce Oddson. 2020. "An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability." *Journal of Cybersecurity* 6 (1): 1–18. https://doi.org/10.1093/cybsec/tyaa023.

Zetter, Kim, 2016. "Why Hospitals Are the Perfect Targets for Ransomware." March 30, 2016, Wired, . https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets.

Zhang, Nan, Yu-an Tan, Chen Yang, and Yuanzhang Li. 2021. "Deep Learning Feature Exploration for Android Malware Detection." *Applied Soft Computing* 102 (January): 107069. https://doi.org/10.1016/j.asoc.2020.107069.

Appendix 1:
Critical Infrastructure Cyber-Attack Incidents' International Sample, 2011-2012

Year	Industry Type	Attack Description	Country	Attack Details
2011	Water and Wastewater Systems	Greenfield Wastewater Treatment Plant intentionally shut down critical systems	United States	SCADA/control systems were intentionally shut down, preventing current wastewater operations from continuing; the tampering of the original security systems and their displayed conditions existed until the start of the backup security systems.
2011	Healthcare and Public Health	Hacker froze operations at pharmaceutical company	United States	Jason Cornish, a former IT employee of Shionogi, Inc. , gained unauthorized access to the computer network. Cornish used a Shiongi user account to access a company server.
2011	Transportation Systems	Computer Glitch Causes Ride Shutdown	United States	The computer systems on the Skywheel ride were not communicating with each other resulting in an error message that stopped the wheel from spinning. The ride was shut down for 17 hours. Passengers were unloaded safely.
2011	Energy	Circuit card shuts down nuclear plant	United States	The Watts Bar Nuclear Plant's Unit 1 reactor shut down. A malfunction in a circuit card on a newly installed computer system that assists the operation of the plant's turbine. The malfunction caused the turbine to trip causing the reactor to shut down.
2011	Transportation Systems	Control system failure causes bridge delays	Guyana	Problems with the bridge control system while opening and closing the bridge resulted in delays for motorists. The bridge typically closes for 90 minutes each day, but the control system problem caused a two-hour delay.
2011	Transportation Systems	Computer glitch causes delayed and canceled flights	United States	The computer glitch resulted in 36 canceled flights and about 100 delayed flights.
2011	Transportation Systems	Computer glitch causes BART train service shutdown	United States	The Bay Area Rapid Transit (BART) system was shut down for about 4 hours due to a computer glitch.
2011	Transportation Systems	Malware a Factor in Spanair Plane Crash	Spain	A Trojan infected computer may not have detected three technical issues that caused the plane to crash shortly after take-off. The crash resulted in the death of 154 passengers. Eighteen passengers survived.
2011	Water and Wastewater Systems	Water Utility Hack Destroys Pump	United States	The control system of the city water utility in Springfield, Illinois was hacked. Hackers gained remote access to the control system causing the system to turn on and off repeatedly leading to the burnout of a water pump.
2012	Water and Wastewater Systems	Wastewater Treatment District Hacked	United States	The former chief financial officer of the Key Largo Wastewater Treatment Distict, Salvatore Zappulla, has been arrested and charged with hacking the district's computer system.
2012	Water and Wastewater Systems	Computer Malfunction Blamed for Major Sewage Spill	United States	A major sewage spill occurred sending 2 million gallons of raw sewage into the Tijuana River. A programmable logic controller failed shutting down pumps and controls.
2012	Critical Infrastructure	Auto Manufacturer Hacked	United States	A computer virus was detected on the network of an automanufacturer. Unknown attackers stole employees' IDs and encrypted passwords after planting a computer virus on the company's computer systems.
2012	Petroleum	Iranian Oil Terminal offline after malware attack	Iran	Iran has been forced to disconnect key oil facilities after suffering a malware attack. The computer virus is believed to have hit the internal computer systems at Iran's oil ministry and its national oil company.
2012	Transportation Systems	Computer Glitch Stops Trains	Philippines	A computer glitch cause the Light Rail Transit Line 2 to stop. The line was down for 30 minutes.
2012	Transportation Systems	Cascade of Computer Crashes Causes Metro System Shutdown	United States	A computer problem caused the shut down of the Montreal metro system for about an hour. The problem started when a computer failure caused a shutdown on the orange line.
2012	Petroleum	Computer Virus Targets Saudi Arabian Oil Company	Saudi Arabia	Saudi Arabia's national oil company, Aramco, said that a cyber attack damaged approximately, 30,000 computers. The attack was aimed at stopping oil and gas production in Saudi Arabia. The company shut down its main internal network for more than a week.
2012	Energy	Computer Glitch Leads to Shutdown of Nuclear Reactor	United States	One of the two nuclear reactors at the Susquehanna Nuclear Powerplant was shut down because a computer system that controls the reactor's water level was not functioning properly.
2012	Petroleum	Shamoon virus knocks out computers at Qatari gas firm RasGas	Qatar	RasGas, the second largest producer of liquified natural gas in the world, was attacked by the Shamoon virus about 2 weeks after a similar attack on Saudi Aramco.

Appendix 2:
Sample of Ransomware Attacks Reported in the Healthcare Sector, 2015-2017

Primary CI Sector targeted	Year	Organization	Location	Modus operandi information	Duration (days, unless specified)	Ransom
Healthcare and Public Health	2015	Christopher Rural Health	USA		2	hundreds of dollars
Healthcare and Public Health	2015	The Arc of Winnebago, Boone and Ogle Counties	USA	CryptoWall	3	$1,400
Healthcare and Public Health	2016	Titus Regional Medical Center	USA		10	
Healthcare and Public Health	2016	Hollywood Presbyterian Medical Center	USA		10	$17,000
Healthcare and Public Health	2016	Lukas Hospital in Germany	Germany		weeks	
Healthcare and Public Health	2016	Klinikum Arnsberg hospital	Germany		1	
Healthcare and Public Health	2016	Los Angeles County Health Department	USA			
Healthcare and Public Health	2016	The Ottawa Hospital	Canada			
Healthcare and Public Health	2016	Henderson Methodist Hospital	USA	Locky	3	$1,600
Healthcare and Public Health	2016	Prime Healthcare Services	USA		days	$17,000
Healthcare and Public Health	2016	MedStar Health Baltimore	USA	Samsam	5	$1,250 - $18,500
Healthcare and Public Health	2016	DeKalb Health Auburn	USA		1-2 weeks	
Healthcare and Public Health	2016	Kansas Heart Hospital	USA		6	
Healthcare and Public Health	2016	Urgent Care Clinic of Oxford	USA			
Healthcare and Public Health	2016	University Gastroenterology	USA			
Healthcare and Public Health	2016	Marin General Healthcare District and Prima Medical Group	USA		1-2 weeks + permanent data loss	
Healthcare and Public Health	2016	New Jersey Spine Center	USA			
Healthcare and Public Health	2016	Keck Medicine	USA			
Healthcare and Public Health	2016	Rainbow Children's Clinic	USA		Unspecified some data never recovered	
Healthcare and Public Health	2016	Appalachian Regional Healthcare	USA		3 weeks	
Healthcare and Public Health	2016	Saint Francis Health System	USA			$14,400
Healthcare and Public Health	2016	Northern Lincolnshire & Goole NHS Foundation Trust	United Kingdom			
Healthcare and Public Health	2016	ARCare	USA		31 hours	about $1,500
Healthcare and Public Health	2017	Erie County Medical Center	USA		5 weeks	$44,000
Healthcare and Public Health	2017	National Health Service (NHS) UK	United Kingdom	WannaCry	3 days	
Healthcare and Public Health	2017	NHS Lanarkshire board hospitals	Scotland	BitPaymer	4	
Healthcare and Public Health	2017	Emory Healthcare	USA		year(s)	about $2,700
Healthcare and Public Health	2018	Hancock Health	USA	Samsam	4 days	$45,000-55,000
Healthcare and Public Health	2018	Adams Memorial Hospital, Indiana	USA			
Healthcare and Public Health	2018	Allscripts Healthcare Solutions, Inc.	USA	Samsam		
Healthcare and Public Health	2018	MN Associates in Psychiatry and Psychology	USA	TripleM		about $27000
Healthcare and Public Health	2018	Blue Springs Family Care	USA			
Healthcare and Public Health	2018	LabCorp	USA	Samsam	1 week	
Healthcare and Public Health	2018	Thundermist Health Center	USA			

Appendix tables' sources, also included in Bibliography:

https://fortune.com/2016/05/07/health-care-ransomware/ (Hackett, 2016)

https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html (Winton, 2016)

https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ (Zetter, 2016)

STRATEGIC DIALOGUE

– Lieutenant General (r.) Virgil BĂLĂCEANU, PhD,
President of the Romanian Reserve Officers Association –

I. The Romanian Reserve Officers Association (AORR) – a think-tank in support of the Ministry of National Defence (MoND) and Chief of Defence's (CHOD) decisional act

Strategic Impact: *Does the AORR's mission include think-tank tasks?*

Virgil Bălăceanu: First and foremost, AORR aims to be a think-tank on security and defence issues. Being a NGO, we have no decisional role, but rather an advisory role. However, our strength lies in our experience and our ability to envision and why not, innovate. One main characteristic of the AORR is its coherent thinking and acting in all its' diversity, as it reunites retired generals and officers, volunteer reserves of all personnel categories, higher education graduates that have completed the short-term military training and civilians taking an interest in defence and security. This diversity represents AORR's main strength as a think-tank.

S.I.: *Is AORR built to support the military decision-making process?*

V.B.: AORR definitely supports the decision-making process of the military, not only by its 'consistent presence in the academic and training areas, on topics related to defence and security issues, but also by its' direct involvement in the strategic defence analysis developed by the Defence Staff or the work groups established following our proposal, inside the Personnel and Mobilization Directorate and the Training and Doctrine Directorate. These work groups deal with the volunteer reserves in relation to proposals for the development of the National Military Mobility Strategy.

S.I.: *What is the link between AORR and MoND and CHOD?*

V.B.: An agreement was recently signed between the AOOR and the Ministry of National Defence, as proof of the mutually beneficial relation in working together towards common goals.

S.I.: *How important is the permanent membership status of AORR within the Interallied Confederation of Reserve Officers (CIOR) in NATO?*

V.B.: Since its inception, AORR has played an active role as a permanent member of CIOR (Interallied Confederation of Reserve Officers in NATO), overcoming critical times when we got suspended for not being able to pay the membership fee.

During the past years we have been actively involved in the CIOR's Executive Council, in various CIOR Committees and specific Confederation actions.

As such, teams representing AORR took part in the MILCOMP (Military Competition), Romania organised the 2022 YROS (Young Reserve Officers Seminar) and is involved in organising the 2024 seminar, we also had reserve officers participating in the second edition of the YROW (Young Reserve Officers Workshop). Our aim is the 2028-2030 CIOR presidency, alongside France, the CIMEX exercises, the foreign language courses being organised by CLA (CIOR Language Academy), with instructors and students, having more teams take part in the MILCOMP. As a side note, inspired by MICLOMP, we intend on creating a Reserve Officers Cup in Romania.

II. The Romanian Armed Forces' Reserve – challenges and realities

S.I.: *Does Romania have truly efficient Reserves to support Active Forces in case of a major conflict?*

V.B.: Romania is deficient in terms of having an adequate number of well-trained reserve forces that could support the active forces in dealing with a potential threat. Post 1997, all the political and military decisions aimed to resize the Military as per NATO requirements and standards.

In 2007, when the mandatory military service was postponed, three years after Romania became a part of NATO, the issue of reserve forces, their procurement and modernisation were totally ignored, on the grounds that expeditionary forces were in no need of permanent, young and well-trained reserve forces.

S.I.: *Do you consider that the provisions of the Law no. 446/2006 on the preparation of the population for defence and of the Law no. 477 of 2003 on the preparation of the national economy and the territory for defence are effective in the current circumstances and produce the desired effects?*

V.B.: These provisions are certainly outdated and to make matters even worse, its amendments are lagging, especially when it comes to the population defence readiness programmes, establishing the volunteer military service, training for the

reserve forces that have completed military service prior to 2007 and pre-military training for the youth. Romania is missing a territorial defence doctrine integrated with the collective defence and overlooks population defence readiness, as well as economy and territorial defence readiness, the three pillars of national resilience.

S.I.: *Do we expect any national considerations to increase the Reserve Force in the near future, as a lesson identified from the Ukrainian War?*

V.B.: The War in Ukraine will determine fundamental changes in Romania and other NATO countries concerning the reserve forces. We are forced to give greater importance to the two major issues – the reserve forces and the national defence industry. Establishing the Territorial Reserve Infantry Battalions is a first step in the right direction, same as involving the national defence industry in many procurement projects.

S.I.: *How were reservists used in the COVID-19 pandemic?*

V.B.: During the COVID-19 pandemic the reserve forces were not called upon, except for some medical reservists. However, they were actively involved in combating the negative effects, one example being AORR donating supplies not only to Romanian hospitals but also to schools in the Republic of Moldova.

III. The Voluntary Military Service and its feasibility within the Romanian Armed Forces' Operational Reserve

S.I.: *In the current security context, in your opinion, what is the optimal recruitment solution for Romania that you consider most effective in terms of the cost-benefit binomial: voluntary military service or conscription? Or, perhaps, a hybrid formula resulting from combining them? Please consider the answer also taking into account the fact that there is no interest from the civilian population in voluntary military service.*

V.B.: Although we cannot state that the 2017-2022 selection within the recruitment process for the volunteer reserves was a success, as the numbers reached only about 20% of those planned and budgeted, at this stage we can still improve the situation by intensifying the volunteer reserve forces recruitment campaigns, amending the Law dealing with the population defence readiness and establishing the 4-month volunteer military service. A welcomed addition could be establishing a training programme based on the American ROTC (Reserve Officers Training Corps). If these measures would prove to be inefficient in the next five to ten years, a hybrid volunteer reserve-mandatory service system could be an alternative.

S.I.: *Do the current voluntary reservists have real military career opportunities after their first tour of duty for retaining perspectives (advancement in the next military rank and job promotion)?*

V.B.: The lack of interest for the reserve corps is also caused by the fact that the MoND did not make use of the legislative framework concerning the reserve forces training, promotions, switching corps during fulfilling their contract or moving from one unit to another. The reserve forces are far from being a selection base for the active forces. The system needs radical improvement in various areas, first and foremost when it comes to the attitude and acceptance towards reserve forces, seeing as the relation is not always one of comradeship.

S.I.: *How efficient is the military education and training system for voluntary reservists?*

V.B.: On the one hand, seeing as the 15 days of annual training are the bare minimum in order to be able to retain information and build the necessary skills, at least half of it must be dedicated to tactical exercises, especially when it comes to firearms training.

On the other hand, there is little to no possibility of voluntary reservists to attend the national military education and training system. Therefore, AORR provides a lot of opportunities for young reserve officers to be trained via CIOR's organised courses, such as CLA, YROW, YROS or MILCOMP.

IV. The Procurement Programmes and the Defence Industry

S.I.: *How is the defence industry anchored to the realities of the national security and the European and Euro-Atlantic development perspectives?*

V.B.: The National Defence Industry, especially that owned by the state, has a limited contribution to Romania's procurement programmes. There is a huge gap between procurement spending and investing in the defence industry. The offset law is yet to be amended, and cannot be put to good use. The private defence sector has slightly better results, however it cannot compete with the financial power, lobby and production flow of the multinational corporations, as we are missing a protection and support system for the private defence industry.

S.I.: *Do the military operations carried out in Ukraine, which are mainly based on land capabilities, require the urgent revitalisation of the national defence industry and the programmes to equip Romania's Land Forces with modern capabilities?*

V.B.: The War in Ukraine brings to attention not only the manoeuvring warfare but also the mechanised war and the war of attrition. The equipment must correspond to the specificities of the European landscape and to the new rules regarding mobility. Prior to 1990, Romania's defence industry was "total war" oriented, and as such it is now unable to provide equipment and maintenance specific to fighting a war on Romania's territory. This is a crucial reason for investing and enforcing some protectionist policies, in order to at least have the ability to build components of military equipment, manufacture ammunition and be able to ensure total maintenance of foreign equipment.

S.I.: *Do you consider that the current procurement programmes are realistic for facing all future risks and threats for the national security?*

V.B.: Current procurement programmes are appropriate not only when talking about the need for modernisation but also taking into consideration lessons learned from the War in Ukraine. However, we have also planned Multirole Corvettes and Frigate Modernisation programmes, in stand by for some time now. This indifference of those in charge towards providing for the defence of Romania is extremely hard to understand and difficult to tolerate. Not to mention the newest trends of UASs, AI, robotics and human performance modification projects.

V. The State Military Pension System – between collapse and reform

S.I.: *Why do you consider the State Military Pension System is so debated in Romanian society and a 'hot potato' on the agenda of each political party?*

V.B.: The topic of military pensions became not only an important point for the political parties but also a focal point for the media. Starting with 2010, we have witnessed a mayhem that has reached new proportions in the last two years. It is in fact a direct attack on the Military, with its active and reserve components.

S.I.: *How is the military pension system organised in other NATO and EU Member States?*

V.B.: Romania tried to align itself with NATO and UE military pension systems, especially after becoming a NATO member. Over time, however, wrong political decisions have taken us further and further away from these systems.

S.I.: *How beneficial do you consider the proposed amendments to the law on special pensions to be (increasing the retirement age to 65 in stages, until 2035, for*

military personnel, surtaxing special pensions by 30% for the part of pension income that exceeds the level of salary earnings gross environment, reducing the number of beneficiaries of service pensions by excluding some categories of staff such as employees assigned to executive positions within diplomatic missions etc.) for the Romanian Military personnel and the attractiveness of the military profession to young people?

V.B.: Up until military state pensions came to be considered special pensions, the system was already facing serious issues, such as updating the pensions, freezing them, confiscating the additional pension that the military had contributed to, refusing to acknowledge the contribution of those that continued working in the civilian sector, after retiring, together with a major discrepancy between similar pensions for the same position, rank, and seniority. The debates concerning the military pensions as special pensions came as a shock to reservists, perceiving them as an attack on their honour and dignity and on the Military as a whole.

The proposed measures, regarding the over taxation of military pensions do not apply righteous principles for all the pensioners and raise a very important issue regarding the retirement age of 65, which will have an aging effect on military echelons that execute missions as their main purpose. As a direct consequence, they will simply not be able to physically accomplish them.

The uncertainty and abusive practices mean that fewer young people are considering a career in the military, as shown by the statistics for the previous two years.

VI. Ukraine under the sign of Mars

S.I.: *Do the strategic documents, such as the National Defense Strategy, the White Paper of Defence and the Military Strategy, still correspond to the current characteristics of the security environment (an ongoing war on Romania's borders)?*

V.B.: Looking at the Russian threat, all the strategic documents require a profound update, as they were developed on a different basis of defence and security at that time, focused on national territorial defence.

S.I.: *It is a known fact that the Russian Federation is also waging an information war in Ukraine. Its disinformation campaigns are also targeting NATO and EU member states, including Romania. How do you assess the measures taken by NATO and the EU – applicable to our country as well – to counter disinformation? And, to the extent that you can provide an answer, how do you assess Ukraine's resilience to Russian propaganda and disinformation?*

V.B.: The so-called Sputnik movement is largely present in NATO and UE countries, including Romania, with their disinformation and pro-Russian propaganda. The effects are obvious, as our institutions grow weaker through campaigns of depreciation, through the lack of proper governing and the lack of a societal security culture.

Ukraine is successfully responding to these campaigns, through their own disinformation strategies that seem to be superior to the Russian ones. When fighting disinformation, one needs to defend but also attack, this is why we are talking about cyber defence as-well as cyber-attacks.

S.I.: *Are the Romanian Armed Forces prepared for a possible escalation of the conflict in Ukraine?*

V.B.: The Romanian Armed Forces are ready for a possible escalation of the conflict, however they are not ready for a possible generalisation.

S.I.: *What are Romania's options in case of an unwanted expansion of the conflict from Ukraine to the Republic of Moldova?*

V.B.: Our options when it comes to a possible spread of the conflict towards the Republic of Moldova need to take into consideration the following elements: sending weaponry, ammunition and equipment, providing intelligence, early warning, training for Moldovan soldiers, medical assistance, hosting refugees, financial support, energy support and food aid.

GUIDE FOR AUTHORS

We welcome those interested in publishing articles in the academic journal *Strategic Impact*, while subjecting their attention towards aspects to consider upon drafting their articles. **Starting with issue no. 1/2023, the journal shall be published in the English language only!**

MAIN SELECTION CRITERIA are the following:

- ✓ **Compliance with the thematic area of the journal – security and strategic studies** and the following topics: political-military topical aspects, trends and perspectives in security, defence, geopolitics and geostrategies, international relations, intelligence, information society, peace and war, conflict management, military strategy, cyber-security;
- ✓ **Originality** of the paper – own argumentation; novelty character – not priorly published;
- ✓ **Quality of the scientific content** – neutral, objective style, argumentation of statements and mentioning of all references used;
- ✓ **A relevant bibliography**, comprising recent and prestigious specialized works, including books, presented according to herein model;
- ✓ **English** language shall meet academic standards (British or American usage is accepted, but not a mixture of these).
- ✓ **Adequacy to the editorial standards adopted by the journal.**

EDITING NORMS

- ✓ **Article length** may vary between **6 and 12 pages** (25.000 - 50.000 characters), including bibliography, tables and figures, if any.
- ✓ **Page settings**: margins – 2 cm, A 4 format.
- ✓ The article shall be written in **Times New Roman font, size 12, one-line spacing.**
- ✓ The document shall be saved as Word (.doc/.docx). The name of the document shall contain the author's name.

ARTICLE STRUCTURE

- ✓ **Title** (centred, capital, bold characters, font 24).
- ✓ **A short presentation of the author**, comprising the following elements: given name, last name (the latter shall be written in capital letters, to avoid

confusion), main institutional affiliation and position held, military rank, academic title, scientific title (PhD title or PhD Candidate – domain and university), city and country of residence, e-mail address.

- ✓ A relevant **abstract**, not to exceed 150 words (italic characters)
- ✓ 6-8 relevant **keywords** (italic characters)
- ✓ **Introduction / preliminary considerations**
- ✓ **2 - 4 chapters** (numbered, starting with 1) (subchapters if applicable)
- ✓ **Conclusions**.
- ✓ **Tables / graphics / figures**, if they are useful for the argumentation, with reference made in the text. They shall be also sent in .jpeg /.png/.tiff format as well.

In the case of tables, please mention above "**Table no. X**: Title", while in the case of figures there shall be mentioned below (e.g. maps, etc.), "**Figure no. X:** Title" and the source, if applicable, shall be mentioned in a footnote.

REFERENCES

It is academic common knowledge that in the Abstract and Conclusions there shall not be inserted any references.

The article shall have references and bibliography, in the form seen below. Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case (e.g. in the case of Cyrillic, Arabic characters, etc.). Please provide English translation for all sources in other languages.

The article will comprise in-text citation and bibliography (in alphabetical order), according to The Chicago Manual of Style[1], as in examples below:

BOOK

Reference list entries (in alphabetical order)

Grazer, Brian, and Charles Fishman. 2015. A Curious Mind: The Secret to a Bigger Life. New York: Simon & Schuster.

Smith, Zadie. 2016. Swing Time. New York: Penguin Press.

In-text citation

(Grazer and Fishman 2015, 12)

(Smith 2016, 315–16)

[1] URL: https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

CHAPTER OF AN EDITED BOOK

In the reference list, include the page range for the chapter. In the text, cite specific pages.

Reference list entry

Thoreau, Henry David. 2016. "Walking." *In The Making of the American Essay*, edited by John D'Agata, 167–95. Minneapolis: Graywolf Press.

In-text citation

(Thoreau 2016, 177–78)

ARTICLE

In the reference list, include page range for the whole article. In the text, cite specific page numbers. For article consulted online, include a URL or the name of the database in the reference list entry. Many journal articles list a DOI (Digital Object Identifier). A DOI forms a permanent URL that begins https://doi.org/. This URL is preferable to the URL that appears in your browser's address bar.

Reference list entries (in alphabetical order)

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. "Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. "Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

In-text citation

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017, 95)

WEBSITE CONTENT

Reference list entries (in alphabetical order)

Bouman, Katie. 2016. "How to Take a Picture of a Black Hole." Filmed November 2016 at TEDxBeaconStreet, Brookline, MA. Video, 12:51. https://www.ted.com/talks/katie_bouman_what_does_a_black_hole_look_like

Google. 2017. "Privacy Policy." Privacy & Terms. Last modified April 17, 2017. https://www.google.com/policies/privacy/

Yale University. n.d. "About Yale: Yale Facts." Accessed May 1, 2017. https://www.yale.edu/about-yale/yale-facts

Citare în text

(Bouman 2016)

(Google 2017)

(Yale University, n.d.)

NEWS OR MAGAZINE ARTICLES

Articles from newspapers or news sites, magazines, blogs, and like are cited similarly. In the reference list, it can be helpful to repeat the year with sources that are cited also by month and day. If you consulted the article online, include a URL or the name of the databases.

Reference list entries (in alphabetical order)

Manjoo, Farhad. 2017. "Snap Makes a Bet on the Cultural Supremacy of the Camera." *New York Times*, March 8, 2017. https://www.nytimes.com/2017/03/08/technology/snap-makes-a-bet-on-the-cultural-supremacy-of-the-camera.html

Mead, Rebecca. 2017. "The Prophet of Dystopia." *New Yorker*, April 17, 2017.

Pai, Tanya. 2017. "The Squishy, Sugary History of Peeps." *Vox*, April 11, 2017. http://www.vox.com/culture/2017/4/11/15209084/peeps-easter

In-text citation

(Manjoo 2017)

(Mead 2017, 43)

(Pai 2017)

For more examples, please consult The Chicago Manual of Style.

SCIENTIFIC EVALUATION PROCESS is developed according to the principle *double blind peer review*, by university teaching staff and scientific researchers with expertise in the field of the article. The author's identity is not known by evaluators and the name of the evaluators is not made known to authors.

Authors are informed of the conclusions of the evaluation report, which represent the argument for accepting/rejecting an article.

Consequently to the evaluation, there are three possibilities:

a) the article is accepted for publication as such or with minor changes;

b) the article may be published if the author makes recommended improvements (of content or of linguistic nature);

c) the article is rejected.

Previous to scientific evaluation, articles are subject to an *antiplagiarism analysis*.

DEADLINES:

All authors will send their articles in English to the editor's e-mail address, **impactstrategic@unap.ro**.

We welcome articles all year round.

NOTA BENE:

Authors are not required any fees for publication and are not retributed.

By submitting their materials for evaluation and publication, the authors acknowledge that they have not published their works so far and that they possess full copyrights for them.

Parts derived from other publications should have proper references.

Authors bear full responsibility for the content of their works and for ***non-disclosure of classified information*** – according to respective law regulations.

Editors reserve the right to request authors or to make any changes considered necessary. Authors give their consent to possible changes of their articles, resulting from review processes, language corrections and other actions regarding editing of materials. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Authors are fully responsible for their articles' content, according to the provisions of *Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation*.

Failing to comply with these rules shall trigger article's rejection. Sending an article to the editor implies the author's agreement on all aspects mentioned above.

For more details on our publication, you can access our site, http://cssas.unap.ro/en/periodicals.htm or contact the editors at impactstrategic@unap.ro

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Layout editor: Gabriela CHIRCORIAN

The publication consists of 98 pages.

"Carol I" National Defence University Printing House
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
E-mail: editura@unap.ro
Tel: 021/319.40.80/215

Nr. 663/28.09.2023 C. 148/2023