National Institute for Intelligence Studies

RISR No. 26 – 2021

ROMANIAN INTELLIGENCE STUDIES REVIEW

EDITURA ANIMV

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 26-2021

The articles published in this volume were proposed by
experts, analysts, practitioners, academics and researchers for the XXV edition
of the *Intelligence in the Knowledge Society* international conference.

The *Romanian Intelligence Studies Review* is an open access academic journal with scientific prestige acknowledged by the National Council for the Validation of University Titles, Diplomas and Certificates (CNADTCU), indexed in the international databases CEEOL and EBSCO.

Bucharest
2021

CONTENT

#COVINTELL – CORONAVIRUS AND THE SECURITY AND INTELLIGENCE SECTOR

MEDICAL INTELLIGENCE AND ITS PERSPECTIVES IN THE POST COVID-19 ERA

Nenad S. KOKOŠKOV*

Abstract:

In its basic thesis, this paper presents medical intelligence (MEDINT) as a specific platform of intelligence work, its historical development, and transfer from the military to the civilian intelligence sector, as well as its transformations from the Cold War period to the present day. It also points out the key features of the application of traditional intelligence methods for the purpose of MEDINT. By setting MEDINT in the context of the current Covid-19 pandemic, we aim to show how the intelligence community contributed to the effective health crisis response by applying certain intelligence tools: epidemiological surveillance, gathering relevant intelligence, targeted counterintelligence and epidemiological contact tracing. The aim of this paper is to anticipate the consequences of the Covid-19 crisis on the future of the global security environment, and to point out new perspectives. It is undeniable that the Covid-19 crisis has imposed the need for medical intelligence to adapt to the new security reality. This process implies not only further development of specific resources (in accordance with MEDINT criteria), but also external connection with professional and academic communities, as well as continuous monitoring of activities that carry a certain risk to public health (dual use research). Eventually, it is especially important for the intelligence sector to build different models of international cooperation that can be crucial in the effective response to global health security threats, such as a pandemic.

Keywords: *MEDINT, Covid-19, public health, security, intelligence, pandemic.*

Introduction

If we take into account the fact that after September 9, 2001, terrorism has become the greatest threat to global security, could the current Covid-2019 pandemic be the turning point in affirmation of biosecurity and, say, bioterrorism at the top of the scale of possible

* Academy of National Security, Belgrade, Serbia, email: nkokoskov@gmail.com

threats to national and global security? Throughout history, the intelligence community has adapted to the security environment, trying to contribute to the more efficient work of political leaders in the protection of national interests. Medical Intelligence (MEDINT), as a specific intelligence category, is aimed at anticipation, prevention, detection, identification and counteraction to health risks and threats. The aim of this paper is not to deal with the securitization of public health phenomena, but to point out the key contributions and importance of medical intelligence primarily to the pandemic as a security threat. In that sense, the Covid-19 experiences are very important in the validation of modern intelligence and security systems as a valuable national resource in the prevention and containment of a pandemic outbreak, as well as in the subsequent damage control.

MEDINT

MEDINT is a specific form of intelligence that essentially deals with the phenomenon of human health in various security, military, political and social contexts. The ultimate goal of MEDINT is to provide quality and timely intelligence products to various segments of the state's management apparatus, which translates into better management decisions. In a holistic sense, MEDINT can be defined as "the application of medical and biological knowledge to national defence" (Jarcho, 1991, p. 501). Also, MEDINT can be defined as "A systematic process of collection and analysis of health hazards; health threats; health risks & medical capabilities in a specific area" (La Gioia, 2015). According to the US Ministry of Defence, MEDINT is defined as "category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors" (US DOD Dictionary, 2021, p. 139). In addition, NATO provides the following general definition of MEDINT: "the product of the processing of medical, bio-scientific, epidemiological, environmental and other information related to human or animal health. This intelligence, being of a specific

technical nature, requires informed medical expertise during its direction and processing within the intelligence cycle". (NATO, 2011, p. 1-21)

A timeline of MEDINT

Following the historical development of MEDINT, it has evolved in accordance with the security environment, the available resources of intelligence organisations, but also the needs of end users of intelligence products. MEDINT originally belonged to military intelligence. At the same time, the standard action of the military intelligence community towards the threat of biological weapons is primarily related to gathering information on foreign military systems, equipment and means, intentions for application of biological weapons, as well as for assessing defensive capacities (epidemiological characteristics, development of public health infrastructure etc.) (Kauffman, 2001, p. 11-13). Today, the military MEDINT supports the engagement of military personnel in peacekeeping missions or conflict hotspots, focusing, in terms of intelligence, on assessing and analysing the existing medical infrastructure "in the field", as well as the potential health risks for military personnel and the health risks for their environment after returning to the home country.

The transfer of MEDINT from military to civilian intelligence structures began after World War II and expanded its areas of operation to monitoring scientific research and development, civil health and numerous issues of importance for public health. (Clemente 2016, p. 282). The end of the Cold War along with multi-polarity in the global distribution of political, diplomatic and military power led to the transformation of the traditional concept of warfare into new forms of conflict with a more dominant asymmetry of the participant's power. In that sense, classical warfare, with the use of conventional weapons, was no longer the dominant form of security threat. Hence, the traditional application of MEDINT, as part of the legacy of the Second World War and the later bipolar division of the world, had to adapt to new subjects, new forms and means of endangerment.

After September 11, 2001, acquired experiences with anthrax letters in the USA, intelligence reports on Al Qaeda's intentions and

capabilities to obtain and to use biological and chemical weapons, and episodes with the Aum Shinrikyo apocalyptic sect in Japan, new security actors as potential users of biological weapons were promoted (Leitenberg, 2005). The largest national intelligence organisations have proportionally developed their own resources in the domain of medical intelligence. Finally, current experiences during Covid-19 impose the need for further transformation and adaptation of intelligence communities around the world, with the medical segment of intelligence systems gaining in importance.

Traditional collection methods and MEDINT

MEDINT exploits all traditional methods and techniques of modern intelligence in the process of gathering intelligence and data. However, the choice of method and its application depend on what is being investigated, who is the target of intelligence processing, what are the requirements of the final consumer of the report, and what resources are available?

Open source intelligence (OSINT), as a method of intelligence, is used in collecting various publicly available data, their analytical processing and subsequent preparing of bio-risk assessments reports with possible prediction of events that could pose a threat to public health and national security. In this regard, the largest security intelligence communities utilize their resources in identifying and analysing security indicators that are important for the production of quality intelligence reports, namely: activities in research centres and institutes dealing with biological agents, application and transfer of dual-use technology, equipment and products, analysis of the development and capacity of health infrastructure in other countries, etc. (Clemente 2016, p. 285-286). A special branch of OSINT is aimed at monitoring and analysing publicly available information regarding epidemiological processes in the world that are important for national security. Therefore, there is an interesting opinion advocated by Walsh who claims that “epidemiology is one critical scientific discipline, where the security community requires information in order to understand how and why disease is distributed across populations of interests, particularly if there are suspicious arising from other intelligence

sources that such distributions may be result of an intentional criminal act" (Walsh, 2018, p. 112).

When we talk about OSINT intelligence sources, a special significance is given to various, publicly available, scientific and professional publications that are relevant for biosecurity. In this sense, Walsh points to another important feature of OSINT sources in medical intelligence, and that is the contribution of the scientific community in understanding the various impacts on public health and national security. "So it is clear that law enforcement agencies and intelligence agencies need to engage with this very broad scientific community for their expertise (e.g. molecular biology, virology, microbiology, public or animal health) on who, what and how of bio-threats and risks." (Walsh, 2018, p. 110).

Apart from open source intelligence, diverse techniques of SIGINT methods have also found their place in collecting medical intelligence. However, when we talk about applying SIGINT techniques, there are some opinions according to which they are the least effective and significant in monitoring the outbreak and spread of infectious diseases. This claim is argued not only by sensitive ethical and legal issues, but also with the disproportionate consumption of intelligence resources (Bernard et al., 2018, p. 511-512). Although, the latest experiences in usage of certain SIGINT tools (monitoring the contacts of infected individuals and digital communications surveillance) applied in the suppression of the Covid-19 pandemic seem to refute Bernard's claims (which will be discussed below). Finally, the application of certain SIGINT techniques (interception of communications or monitoring of activities on social media) can be more than useful in early detection and prevention of bio threats, such as potential risk of intentional use of biological agents by malicious organizations, groups or individuals.

The use of human Intelligence (HUMINT), the oldest form of intelligence, might have a very significant contribution in obtaining quality MEDINT products. The potential targets of HUMINT can be scientific (dual-use) research institutions dealing with high-risk biological agents or military biological research facilities of foreign states. Also, recruiting agents in terrorist, criminal or various extremist

organizations can be crucial in terms of early identification of a security threat based on the use of biological weapons or endangering public health by other means. Espionage is also crucial for accurate assessment of the intentions and objective capabilities of the enemy. The importance of HUMINT is particularly important in cases where other intelligence methods show less penetrability, accessibility or reliability. Hence, HUMINT can provide intelligence verifications of certain indications or speculations that incidentally accompany the Covid-19 pandemic. Comparing the role of OSINT resources, social networks and SIGINT methods of intelligence, Bernard et al. came to the conclusion "that there is a place for OSINT and SIGINT in the detection and reporting of outbreaks. However, such tools are not sufficient on their own and must be corroborated for the intelligence to be relevant and actionable". (Bernard et al. 2018, p. 509)

MEDINT and the Pandemic

In the operational-tactical sense, all the activities of intelligence and security services regarding the pandemic can be systematized into two functional segments: PRE-exposure and POST-exposure. In this setting, intelligence activities are observed exclusively in accordance with one time coordinate, and that is the moment of occurrence of the negative event itself (the beginning of the pandemic). The first (pre-exposure segment) is therefore important in the prevention and prediction of infectious disease, with the development of hypothetical models of its possible course and consequences, while the second is aimed at reducing its consequences and controlling the damage. (Kokoškov & Ristanović, 2021, p. 27) POST-exposure intelligence activities begin when a negative event (epidemic/pandemic outbreak) has occurred. Regardless of what caused the epidemic/pandemic (natural or artificial processes), the response to it will be essentially the same. It will be conducted by the national public health system in cooperation with other entities within the state capacities. The goal of these activities will be aimed restrain the negative process and eliminating its consequences.

The role of intelligence communities (MEDINT) during the Covid-19 crisis

The current pandemic caused by SARS-CoV-2 presents a globally distributed infectious disease that has caused massive human diseases as well as numerous functional disturbances in the public health, economic, cultural and every other segment of societies. It is a very convincing and well-argued example of the extent to which the global public health crisis is becoming a geopolitical and a security problem.

By analysing the contributions of security and intelligence agencies in the fight against Covid-19, Walton points to four key courses of action (Walton, 2020). The first one deals with health intelligence monitoring and evaluation of epidemiological processes that are important for national security. The goal of this activity is to timely, accurately and clearly inform political leaders about potential biological threats, their possible course and impact. It can be applied both in the pre-exposure phase and after the outbreak of a pandemic.

The second direction of intelligence action towards the pandemic presents the classic espionage aimed at gathering secret data and information with the aim of revealing the intentions, but also assessing the capabilities of foreign states. One of the most intriguing questions that accompany the Covid-19 crisis is related to the origin of the virus. Apart from the health perspective, this question also encompasses a security, and even a geopolitical connotation. Nevertheless, as the pandemic progressed, interest in information related to the pandemic expanded to the efficacy of certain drugs, research and development of new vaccines and their efficacy and safety, global distribution of new strains of SARS-CoV-2, and others. In this context, it is realistic that some national intelligence services have been actively working to provide information and intelligence assessments that have helped their national leaders in crisis management.

The third direction is especially important because it is aimed at opposing the placement of untruths and misinformation and basically has a counter-intelligence character. It will be discussed in more detail below.

Finally, the fourth model is based on the application of technical measures to monitor the contacts of persons who pose a potential risk

for the spread of infection in the population. According to the WHO, epidemiological contact tracing is one of the crucial health measures in the suppression of contact-communicable infectious diseases (World Health Organization, 2017). In this way, people who have been exposed to the virus and who pose a health risk in the further spread of the infection need to be identified. Hence, "For contact tracing to be an effective public health measure requires most secondary cases to be discovered and isolated before they become infectious" (Keeling, 2020, p. 865). In a research study conducted by the University of Oxford, it was scientifically proven that the traditional way of manually monitoring contact tracing in the case of SARS-CoV-2 is not efficient and fast enough to monitor the behaviour of the current pandemic, suggesting the use of modern digital tools (Ferretti et al., 2020, p. 4). However, although the application of modern digital techniques in epidemiological surveillance has proven to be effective, it has nevertheless initiated very sensitive ethical and legal discussions, which may affect the modality and scope of their application in the future.

Counterintelligence activities during Covid-19

The activities of national intelligence services during the pandemic also play a significant role in the counter-intelligence sense. In the preventive segment, this action is primarily focused on protecting their own sensitive security information and concealing the activities of national entities in legitimate dual use researches that pose a potential risks to public health and biosafety. However, when a pandemic occurs, post-exposure counterintelligence actions are directed towards the application of denial, deception and disinformation (DDD) techniques. In that sense, constant monitoring of activities on the internet and social media is of key importance. Since these communication spaces have an increasing influence on creating public opinion and attitudes, they could be useful for various abuses and malicious actions. (Kokoškov & Ristanović, 2020, p. 37)

During the Covid-19 crisis, the internet and social media were promoted as one of the most powerful platform for offensive counterintelligence. Conspiracy theories about the origin of the virus, its spreading, the effectiveness of personal protective equipment, the

performances of the virus itself; development, efficiency and (non)harmfulness of vaccines, etc. are topics that have gained a lot of attention on social media. The spread of untruths and misinformation on these topics has greatly influenced the attitudes of the public, the loss of credibility in the states' institutions in general, as well as the efficiency of health crisis management, and finally the course of the pandemic. Back in February 2020, addressing the participants of the Security Conference in Munich, WHO Director A. Gebrejesus warned the audience with the words "We are not only fighting a pandemic, we are also fighting an infodemic" pointing to the huge harmful impact of false information on opposition pandemic. (Ghebreyesus, 2020)

By analysing these complex impacts during a pandemic, Bernard et al. make a very bold claim "We are approaching the fifth phase of bio warfare with a cyber-bio framing."[1] According to Bernard, this latest (fifth) generation of biological weapons, actually represents a synergy of two different detrimental impacts: spreading misinformation combined with public health damage (naturally or intentionally caused human diseases). This creates numerous consequences in terms of undermining social and political stability, compromising state institutions, as well as delegitimizing science and its contribution to controlling the health crisis (Bernard et al., 2021, p. 3-4). Thus, we actually have a combined cyber-bio attack, as a synergy of the harmful effects of information with the action of biological agents. In this context, we can say that the future activities of the intelligence community towards this type of threat are further complicated by the fact that in cyberspace may intertwine the influences and interests not only from opposing (or competing) states, but also other relevant actors (movements, organizations, individuals or corporations). This requires

[1] This thesis is based on a historical overview of the development of the biological weapons (BW) given by Koblentz. According to him, the first generation of BW consists of original microorganisms (easily accessible and unprocessed); the second generation of BW is characterized by the production of small quantities of biological agents and their primitive dissemination, the third is characterized by the use of sophisticated methods of dissemination of previously processed biological agents, and the fourth generation is the result of aplying state-of-the-art biotechnological achievements in production and application. (Koblentz, 2009, p. 203-205)

special attention in the intelligence identification, analysis and qualification of information collected from the internet.

The post Covid-19 era and new security reality

Covid-19 shows us the extent to which states, their public health systems, as well as other segments of critical infrastructure were unprepared for a health crisis such as a pandemic. The same can be said for national security and intelligence communities around the world.

Massive deterioration of health, with numerous psycho-social and other consequences in societies, could have very motivating effects on certain security actors in terms of potential use of biological weapons. This would also point to a very realistic reaffirmation of biological terrorism or bio criminal acts.

When we consider possible use of biological weapons in the future, an interesting thesis was presented by Silke, who claims that "an added concern is that historically it has mainly been religiously-motivated or right-wing terrorist who have been most attracted to using biological weapons, and in the west these are currently the dominant terrorist movements". (Silke, 2020, p. 7) Hence, it is an understandable assumption that in the future, biological weapons can pose a real threat of endangerment by jihadists groups such as the Islamic State or various extreme right-wing organizations. (Silke, 2020, p. 7) In support of the reaffirmation of the use of biological weapons, the observation of Ong and Azman (2020, p. 18-20), who point to the proactive behaviour of right-wing organizations in an attempt to use SARS-CoV-2 during the pandemic, is indicative, while the Islamic State did not encourage its supporters to take these steps.[2]

When we talk about the harmful effects of a pandemic on societies, the economic consequences should not be neglected. Arguably, they will have certain reflections on national security. In that sense, Silke points to another negative aspect of Covid-19 on national security: "Looking ahead in the medium and long term, government

[2] Members of right-wing organizations in a primitive way "weaponized" SARS-CoV-2 by using the sputum of their sick members to contaminate public areas or by coughing and blowing in the face etc.

spending is likely to come under the fiercer stress than in the past decade and pressure on counterterrorism budgets going forward is likely to be more intense. Tied into this, the economic impact of the pandemic is almost certainly going to feed into destabilising parts of the world. Countries with less resources may face even greater crises."(Silke, 2020, p. 8)

The intelligence community in the post Covid-19 era

The future adjustment of the intelligence community in the post Covid-19 era encompasses several directions. First, it is necessary to develop and strengthen MEDINT intelligence resources within intelligence systems. The continuous education of existing staff, but also the introduction of new expert profiles in the intelligence and security structures themselves might be a special challenge. In that context, Kauffman pragmatically suggests: "It is far easier to teach a medical – or life-science expert about intelligence than it is to teach an intelligence officer about medicine or biology" (Kauffman, 2001, p. 23).

Second, the broad spectrum of numerous and diverse factors and entities that affect public health imposes the need to engage the intelligence community with representatives of different professional sectors and disciplines. Accordingly, it is necessary to establish external connections of intelligence structures with entities from different expert sectors and disciplines (epidemiology, ecology, molecular biology, medicine, veterinary medicine etc.), as well as with relevant representatives of the academic community. The importance of such multidisciplinary connection is also pointed out by Bowsher who notes "It is also apparent that the possession of highly capable intelligence services does not currently translate into highly effective health intelligence practice and that this domain requires specific multidisciplinary consideration for further development as a state capability." (Bowsher et al., 2021, p. 437)

Third, security and intelligence monitoring of sensitive research in the field of biotechnology and molecular biology (dual-use) should not be neglected. Their reach, dynamic development, but also increasing availability will increase the risks of bio accident threats, as well as bioterrorism or bio criminal acts.

Fourth, full promotion of international cooperation at the regional and wider international level is necessary. Biological threats usually do not recognize national borders. This is especially evident in the case of a pandemic. International cooperation in the MEDINT domain can be achieved on operational and tactical level (information exchange, education etc.)

Conclusions

The pandemic as a health phenomenon in its genesis, spread, consequences, and in our reactions to it, certainly goes far beyond national frameworks. Non-functional international cooperation manifested through the absence of health solidarity, and non-recognition of common interest in the field of biosecurity are also important lessons of Covid-19. Cooperation between international entities is unavoidable in order to prevent and recognize pandemics and similar health threats in a timely manner. In that sense, one should be aware of the existence of certain cyclical patterns in the behaviour of infectious diseases with epidemic/pandemic potential (SARS, MERS, SARS-2, Ebola etc.). It should be considered as a warning and indication of mostly possible bio-risk of new natural epidemics or pandemic outbreaks.

Whether we talk about pandemics as naturally generated processes or pandemics as a consequence of aimed and malicious actions carried through biological weapons, the intelligence community will have to develop and adapt to the new security reality. In this way, MEDINT has also gained in importance. A special segment of international cooperation concerning endangering the health of the population is the potential risk of bioterrorism and other abuses of biological agents. The post-Covid era will certainly require the establishment of a better and more efficient system to counter bioterrorism through existing and new models of international cooperation. The Council of Europe Committee on Counterterrorism (CDCT) reacted in the midst of the pandemic, pointing out the weaknesses of modern societies towards the pandemic, warning that the global spread of the SARS-CoV-2 virus could increase the risks of possible use of biological weapons by terrorists.

Furthermore, this EU body notes that it is necessary for all 47 member states to commit to training and preparations for a potential terrorist attack with biological weapons (Council of Europe, 2020). Finally, medical intelligence should not be the privilege of the most developed national intelligence services, but a necessity of every modern intelligence system in the world. Covid-19 has undoubtedly become the ultimate security issue for the whole world. In a rather traumatic way, we realized that endangering the public health can be far more than a medical issue. If there was ever any doubt regarding the justification of the existence of MEDINT incorporated within security intelligence systems, it now belongs to the past.

References:

1. Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P., & Sullivan, R. (2018). Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. Zeitschrift fur Gesundheitswissenschaften (Journal of public health), 26(5), 509–514. https://doi.org/10.1007/s10389-018-0899-3

2. Bernard R, Bowsher G, Sullivan R, and Gibson-Fall F. (2021). Disinformation and Epidemics: Anticipating the Next Phase of Bio warfare. Health Security. February 2021, 3-12. http://doi.org/10.1089/hs.2020.0038

3. Bowsher, G.; Milner, C.; Sullivan, R. (2016). Medical intelligence, security and the global health. Journal of the Royal Society of Medicine, Vol. 109, Issue 7, Sage Publishing, UK, 2016, 269-273. DOI: 10.1177/ 0141076816656483

4. Bowsher, G., Bernard, R., & Sullivan, R. (2020). A Health Intelligence Framework for Pandemic Response: Lessons from the UK Experience of COVID-19. Health Security, 18(6). https://doi.org/10.1089/hs.2020.0108

5. Clemente D. Jonathan. (2016). Medical Intelligence. Guide to the Study of Intelligence. The Intelligencer-Journal of Intelligence Studies.

6. The Council of Europe continues working to enhance international co-operation against terrorism, including bioterrorism. Strasbourg. 25/05/2020 https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism

7. Ferretti, Luca et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science, American Association for the Advancement Science, Washington, D.C., Vol. 368, Issue 6491.

8. Ghebreyesus, T. A. (2020). Speech presented at: Munich Security Conference; February 15, 2020. https://www.who.int/director-general/speeches/detail/munich-security-conference

9. Jarcho, Saul. (September/October 1991). Historical Perspectives of Medical Intelligence. Bulletin of the. N.Y. Acad. Med. Vol. 67, No 5, 501-506.

10. Kaufman, D. C. (2001). Medical Intelligence: A Theatre Engagement Tool. Strategy Research Project, Carlisle: United State Army War College, 2001.

11. Koblentz, G. (2009). Living Weapons: Biological Warfare and International Security. Cornell University Press. Retrieved May 9, 2021, from http://www.jstor.org/stable/10.7591/j.ctt7z9s0

12. Кокошков, Ненад, Ристановић, Елизабета (2019). Медицинско обавештајно деловање према истакнутим личностима. Национална безбедност, година 6, број 9/2019, стр. 79-96.

13. Кокошков, Н. Ристановић Е. (2020). Обавештајно-безбедносни рад и пандемија, Национална безбедност, година 7, број 11/2020.

14. Keeling, Matt J., Hollingsworth, Deirdre T., Read, Jonathan M. (2020). The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), J Epidemiol Community Health. 2020, 74, 861-866. https://doi.org/10.1101/2020.02.14.20023036

15. La Gioia, Vicenzo, Col ITAF. (November 5, 2015), Medical Intelligence in Biological Issues. Biosecurity & Biosafety: Future Trends and Solutions. Centro Intelligence Interforze.

16. Leitenberg, Milton. (December 2005). Assessing the Biological Weapons and Bioterrorism Threat. Monograph from the Strategic Studies Institute.

17. NATO. (May 2011). Allied Joint Medical Support Doctrine. (AJP-4.10(A), NSA (MED) 0562(2011)1

18. Office of the Chairman of the Joint Chiefs of Staff. (January 2021). DOD Dictionary of Military and Associated Terms. Washington DC: The Joint Staff.

19. Ong, Kyler, Nur Aziemah, Azman. (2020). Distinguishing between the Extreme Farright and Islamic State's (IS) Calls to Exploit COVID-19. Counter Terrorist Trends and Analyses 12, no. 3. 18-21. doi:10.2307/26915446

20. Silke, Andrew (2020), Pool Re and Cranfield University's professor of Terrorism, Risk & Resilience Commentary. Covid-19 and terrorism: assessing the short and long term impacts. https://www.poolre.co.uk/wp-content/uploads/2020/05/COVID-19-and-Terrorsim-report-V1.pdf

21. Walsh, Patrick F. (2018). Intelligence, Biosecurity and Bioterrorism, Palgrave Macmillan UK.

22. Walton, Calder. (April 2020). Spies Are Fighting a Shadow War against the Coronavirus, Foreign Policy, 3. https://foreignpolicy.com/2020/04/03/coronavirus-pandemic-intelligence-china-russia/

23. World Health Organization (WHO). (May 9, 2017). Contact tracing: What is contact tracing and why is it important? https://www.who.int/features/qa/contact-tracing/en/

SOCIAL ASSISTANCE – PRACTICAL SOLUTION TO ENSURING HEALTH SECURITY IN THE POST PANDEMIC PERIOD

Maria PROCA[*]
Valentina STRATAN[*]

Abstract:

In the field of human security, public attention is often captured by those violent acts, which immediately cause suffering and loss of human lives, such as trafficking in human beings, terrorism or even the pandemic. However, social life also has other aspects that, if the suffering and human loss and/or financial costs would be quantified, could overcome or, at least, reach the same heights as the loss from the threats mentioned above. The incidence of modern society as a source of social risk with impact on personal safety is major. As a result, the number of disadvantaged and vulnerable people is continuously growing, taking into account the SARS COV-2 pandemic. The field of social assistance is closely connected to human security. Thus, approaching the two dimensions in tandem, in terms of setting up strategies and national policies related to social protection, will ensure a reduction in the number of people at risk from vulnerable categories. In addition, this will make it possible for the objective of the Porto Social Summit held on May 7-8, 2021 to be achieved. In its framework, the participants discussed strengthening of the European institutions' commitment to the implementation of the European Pillar of Social Rights, one of their aspects being the reduction of the number of people exposed to the risk of social exclusion.

Keywords: *social assistance, social risk, health security, human security, pandemic.*

[*] Researcher PhD, "Bogdan the Founder of Moldova" National Institute of Security and Intelligence, Republic of Moldova, email: aprodan@mail.ru.

[*] Professor PhD, "Ion Creangă" State Pedagogical University, Republic of Moldova, email: vstratanmd@yahoo.com.

Introduction

The paradigm of human security is based on the idea that the citizen is the referent object of national security, along with the state and the community he/she belongs to. The contemporary reality has once again proved, by a concrete example, that risks often entail consequences for all the three components of national security, not only for one element. It is particularly worrying when an asymmetric threat impacts the social community, the individuals and the states at global level, but the response capacity lacks an adequate strategy, a policy to prevent surprises or operative actions with immediate effect. We are here referring to the COVID-19 pandemic which, apart from the fact that it globally rocked the public health system, has a direct economic and social impact on both national and international security, shaped in quite pessimistic terms. It is therefore difficult to answer the question "who has suffered the most: the citizen itself, the community, or the state overall?" One thing is clear – the health security of the individual has been seriously affected to the point of losing human lives, and the chances for sustainable development of current social communities, including strong economies, have been considerably reduced.

The current study will focus on approaching the area of social assistance from the perspective of presenting a strategic solution with practical applicability for state institutions with competences in the field of ensuring health security. The solution put forward is aimed at reducing the impact of Coronavirus in the post-pandemic period on socially vulnerable people. Provided that the world's states have been caught by the COVID-19 pandemic with no strategy on prevention or counteraction of social asymmetric and pandemic risks, the current social circumstances require an urgent need for the development of a multidimensional long-term policy, looking to counteract the consequences of the aforementioned peril, which affects a huge number of people in terms of physical and mental health and the lack of financing sources. The current study is oriented towards approaching the sphere of social assistance as a component of accomplishment of the health security policy in the post-pandemic period and inviting state institutions to pay a greater attention to this field in terms of providing a structural-strategic solution of practically ensuring human security

beyond the post-pandemic period. It is important to mention from the start that the topic addressed further is only one of the segments suitable to be included in a multidimensional strategy in the field of ensuring the health security in a state, considering that insecurity cannot be approached separately, by fragmentary and independent responses.

Approaching the protection of the person from the interdisciplinary position – human security/human health and social assistance – emphasizes the understanding between the cause and effect of all people's life standard, whatever resources they might have. That is why in our study we have analysed a number of social policies, which reflect the aspects of health security and social assistance.

Aspects of health security in the SARS-COV–2 pandemic period

In the 1980s, the researcher Ulrich Beck explained a new theory in the sociological literature, the theory of "society risk". This notion would further be applied in the field of security studies (Nate, 2014, p. 24). According to this theory, contemporary human communities live in an insecure environment, because modernity generates security risks. The Explanatory Dictionary of the Romanian language defines *risk* as being the probability to overcome a hypothetical threat, and associates it to damages, wastes and lost incomes. In 1994, in the Global Report on human development, the United Nations Organization defined the concept of human security, with its seven component parts: economic security, health security, personal security, political security, food security, environmental security and community security (Gomez and Gasper, n. d., p. 2). The concept defines human security as the human state of safety against famine, diseases, oppression and other chronic threats, as well as protection against sudden and painful daily disturbances. Human security presumes taking into account factors generating insecurity to the individual particularly.

The social scientist Deborah Lupton distinguishes six risk categories that seem to integrate the concerns of the individuals and those of the modern society's institutions (Szabo, 2007, p. 42): "*environmental risks*: pollution, radiation, floods, conflagrations; *risks*

associated with lifestyle: inadequate food consumption, drugs consumption, unprotected sexual contacts, driving styles, stress; *medical risks*: related to medical treatments, consumption of medicines and surgeries, birth or new reproduction technologies; *interpersonal risks*: referring to intimate relations and social interaction, sexual relations, friendship, marriage and parenting; *economic risks:* unemployment, lack of jobs, debts, loans, investments, bankruptcy, property destruction; *criminal risks*: related to the position of a participant to or victim of an illegal activity."

As the range of social risks that might have consequences on the personal security is wide and considering the impact of modernity over the personal security (currently a source of social risk), the risks repercussions associated to an individual lifestyle and deliberate behaviour, we can conclude that the medical condition of an individual encompasses his/her lifestyle, living and environmental conditions, technological progress. In this situation, it is relevant to see how asymmetric risks with impact on health security are prevented, minimized or eliminated, which is primarily the responsibility of the state competent authorities (Stratan and Proca, 2020, p. 241).

The COVID–19 pandemic (from English COrona VIrus Disease-19) is assessed not only as a global health crisis, but also as the biggest challenge that humanity has faced after World War II, affecting all the continents. According to the UN defined concept, the side effects of this phenomenon over individuals could have hybrid incidence on human security. Therefore:

- Health security also refers to the protection of individuals from the threats generated by pandemics and diseases, as a consequence of an inadequate access to health services. Or, to put it differently, the pandemic period influences the physical and psychological condition of the individuals, whether they have been affected by SARS COV-2 or not; and the disruption of the health system generates a real risk for health security similar to the pandemic associated risk.

As a result, according to the data presented by the World Health Organization, the pandemic continues to affect the capacity of health

services in the majority of states, because the human resources are oriented towards answering to the outbreak. The lack of health care assistance is perceived not only amongst the individuals hit by COVID-19, but also amongst patients suffering from other pathologies. In April 2021, more than 90% of the countries reported the interruption of the health care services to a different extent, and around 40% of other states reported a total suspension of primary health care services. (WHO, 2021) Simultaneously, the pandemic entailed psychological consequences on some individuals, as a result of disease, while for other social groups these consequences are the result of a long-lasting anxiety. For example, in the Republic of Moldova, for more than half of the population the isolation, the abundance of home responsibilities and the fear generated by the virus represent an extremely difficult challenge in terms of mental health (UN WOMEN Moldova, 2020).

- Economic security of the person involves the protection of the individual from the hazard generated by poverty and, as a consequence, unemployment. During the pandemic, many people became vulnerable due to the loss of their jobs or incomes, and, as a result, got into the group of risk susceptible to expand the pauperized social category, thus deepening even more the existing social inequality.

According to the International Labour Organization (ILO), the loss of working hours in 2020 was approximately four times higher than during the 2009 financial crisis. In the fourth trimester of 2020, the number of working hours dropped by 4.6% on a worldwide scale, being the equivalent of 130 million full time working places. The global unemployment rate grew up by 33 million in 2020. During previous crises, the loss of working hours on a large scale was usually associated with the increase of unemployment rate. During the COVID-19 crisis, the state of inactivity and the reduced working hours became the major factors for the total loss of working hours. The global employment rate decreased by 2.2% in 2020, in comparison with only 0.2% in the 2008-2009 global financial crisis. Estimated loss from employment income decreased by 8.3% in 2020 as compared with 2019, situation similar to those countries with low income, upper-middle income and high

income. This corresponds to 4.4% of the global GDP in 2019. The reduction of the employment incomes was unequally distributed among employers, confirming the fact that the loss of income is associated with a higher inequality (ILO, 2021).

- Personal security means protection of the individual against physical violence irrespective of its source. Imposing lockdowns has entailed as side effect increased risks for physical or mental violence, sexual abuse in different contexts towards vulnerable persons, women, and children.

A report published by World Vision estimates that as a result of the first three months of global quarantine, the number of children exposed to risks of different kind of violence has grown by 85 million (Stancu, 2020). In the Republic of Moldova, the most affected victims of domestic violence were women rather than men, around 46% of the women having the fear of becoming such victims (UN WOMEN Moldova, 2020). In addition, the access to psychological assistance for stress management in crises was restricted. The switch to online work and education led to an increase in cyber-crimes with impact on personal security: blackmailing individuals after obtaining their personal data, sexual abuse of children etc.

This situation will for sure lead to an increase in the number of vulnerable and marginalized people in each country. In this context, it is worth mentioning the list published in 2019 by the WHO of the 10 global major health threats, as follows:

- *"Air pollution and climate changes* – seven million fatalities annually are caused by diseases such as: cancer, stroke and cardio-respiratory diseases, caused or aggravated as a result of air pollution. Pollution is one of the main causes contributing to global warming, consequently, generating fatalities, such as malaria, diarrhea, malnutrition and insolation;
- *Non–communicable diseases* – cancer, diabetes or cardiovascular diseases (41 million fatalities/year and 71% from the total death global rate). Main *risk factors*: smoking,

sedentary life-style, alcohol consumption, unhealthy diet and air pollution;

- *Global pandemic influenza* – according to the statistics published in November 2018, the flu kills annually up to 650.000 persons;
- *Vulnerable and dangerous environments* – almost a fourth of the population of the globe (1,6 billion) lives in environments vulnerable to risks with impact on human health because of drought, hunger, pandemics or military conflicts;
- *Antimicrobial resistance* – is determined by the long-scale prescription of antibiotics, use of antibiotics on a large scale in agriculture and zootechny. It will be impossible to cure infections such as: pneumonia, tuberculosis, salmonellosis etc.;
- *Hesitation or refusal of vaccination* – a tendency to refuse to be vaccinated is observed, despite the availability of vaccines." (Ro Health Review, 2019)

In the period of reference, the abovementioned factors substantially intensified. Even if the media sources refer to a slight improvement of the indices of environment pollution, in November 2020, the European Environment Agency (EEA) stated that 90% of the inhabitants of the European cities are exposed to pollution in a proportion surpassing the normal air quality indicators (European Environment Agency, 2021). Moreover, the EEA asserts that the individuals disadvantaged in terms of age and social-economic situation are also disproportionally affected by the environmental hazards (Kazmierczak, 2019). The pandemic crisis proved that epidemics can turn the entire globe into a vulnerable environment for the human health and other type of related hazards. Thus, according to the official data presented on 20 April 2021 by the World Health Organization, the total number of fatalities in the pandemic period exceeded 3 million of human lives (WHO, 2021). COVID–19 caused serious and/or lethal complications for those categories of people posing health problems – older people, persons suffering from other diseases while being infected, with a weakened immune system or having non-communicable disorders. How these consequences might manifest remains unknown.

The antimicrobial resistance causes annually around 700,000 fatalities, and this number might increase up to 10 million in 2050. This risk factor will become one of the main causes of death in the European space (Edelstein et. al., 2021). The refusal of vaccination was a debate topic, even at the European Court of Human Rights (ECHR), which stated that imposing vaccination is in principle allowed (DW, 2021). So, all these threats in the context of jeopardizing the health system in the pandemic period will affect a lot of individuals, which might get into the disadvantaged group.

The published literature presents the concepts of human security and health security, referring more to the prevention of risks, irrespective of its source, and touching less the subject referring to reintegration in the social environment of the vulnerable persons in those cases when irrecoverable health consequences are registered.

Why social assistance?

Today, all of us have become witnesses to an unprecedented situation, due to the fact that the pandemic has reduced to a minimum the health security guaranteed by the state and a huge number of people become vulnerable because of the health, psychical or financial problems. All these aftereffects have impacted the health dimension, among others, and have generated human security deficiencies. If social assistance is to be an essential component of human security, due to the fact that these relations are generated by necessity, poverty, fear and at the same time refers to all the persons being in difficult situations because of economic, social, physical and mental reasons (Stratan and Proca, 2020 p. 128), it is necessary to include the medical-social assistance in a national post–COVID strategy for countering pandemic consequences by providing assistance to vulnerable people, beyond mere theory. This fact will contribute to a faster revival of the public health system.

The role of social assistance is to help those people who face difficulties to integrate themselves in the social environment. There is a special group of individuals considered main beneficiaries of social assistance. Among them, the individuals who cannot enjoy their essential and fundamental rights are to be included: the right to

appropriate nutrition, decent housing, health and hygiene services, education, and those not having a stable income or possibilities of self-realization. Social assistance presumes a group of institutions, programs, measures, specialized activities and services aimed to protect and help people, groups and communities being temporary in difficulty, who cannot ensure, by their own forces, a decent life due to economic, social, cultural, biological or psychological reasons.

Social assistance establishes and encourages a *mutually beneficial interaction between individuals and society*, with the aim to raise the social life quality at both personal and family level, and at the level of groups and community as well (Hepworth and Larsen, 1990, p. 644). The reciprocity of the interpersonal relations is one of the main characteristics of social assistance, and offers resources and opportunities for achieving goals and necessities for marginalized individuals and for those being in difficulty because of different reasons.

One of the social assistance paradoxes resides in the fact that, besides its main task of taking care of vulnerable social categories, it is also *responsible for maintaining social balance and existing social order, preventing in such way mass disorders or social crises* (Davies, 1994, p. 39-42). This function is expressed in restorative actions regarding social equity. It is regulated by national legislation on social assistance of each state and any failure to comply with legal provisions may generate the loss of a specific type of social protection. According to Jordan B. (1997), social assistance includes a set of measures used by the society to protect it, by granting compensatory support to marginalized categories of people suffering from the negative consequences of the market economy. From here the main objective of social assistance to support the individuals in difficulty, in order to help them develop their own abilities and competences, so as to achieve the basics for a decent life and a better social functioning. At the same time, the social-vulnerable category of a community is composed of people with low individual and social functioning, who become victims of different social risks against their will. SARS COV-2 is one of the abovementioned risks.

The published literature identifies two types of risks and threats addressed to a person: *"hard" type risks and threats* – international

terrorism, proliferation of weapons of mass destruction, intra-state and interstate conflicts etc.; *"soft" type risks and threats* – environmental degradation, extreme poverty, unemployment, contagious diseases, etc.

Even if the Universal Declaration of Human Rights states the right to subsistence – right to food and fundamental standards of health and well-being, (ONU, 2015, p. 52), and such threats as infectious diseases, unhealthy conditions, famine etc., are essential health insecurity factors to individual health security (UN, 2009, p. 7-11), state authorities tend to consider less the "soft" type risks, as compared to the ones from the former category.

It is important to highlight the main peculiarity of the social assistance, which consists in *intervention and practical support* at both individual and community levels, based on the principle of "action-research". Thus, due to its multiple levels of practical intervention in real life, social assistance gets a special mission of preventing and reducing modern risks (Zamfir, 2019), *including those risks of affecting individuals' health security*. According to the opinion of the Romanian researcher E. Zamfir, social assistance is an environment of medical and social interaction, *a specialized response to the complexity of human bio-psycho-social-cultural life necessities*. From here derives the perspective of an integrated social policy in restoring health security in a state. Thereby, social-medical assistance consists of a complex of activities, together with social and medical services provided at once, aimed at solving the social-medical issues of the individual, unable to ensure his own social needs and to develop his own capabilities to integrate in the society, due to social, economic or psychical reasons. In this respect, it is a priority to render social and medical integrated services to vulnerable people in the environment they live, depending on their specific needs.

Considering that the current issue of the state entities consists in establishing a strategy for overcoming the consequences of the pandemic threats marginalizing a large number of people against their will, it is worth mentioning that, in practice, human security is applied within a society by means of insurance and social assistance as component parts of the social protection state system, often identified as social security. Social assistance plays a significant role not only in identifying the needs of vulnerable individuals, but also in solving their

particular issues through an integrated and multidisciplinary comprehensive approach.

If the main feature of human security consists in protecting the individual by ensuring an efficient management of potential threats that might affect human life, than social assistance is concentrated on simplifying the life of those already affected by different threats, providing to them appropriate support and help. More and more proofs suggest that social risks are not equally distributed within the society, and affect in a disproportionate way the vulnerable and socially disadvantaged categories of population (European Environment Agency, 2021). The socially disadvantaged individuals may be more sensitive to the action of any stress factors, such as environmental, work or psychological factors, as consequence of pre-existing affections, malnutrition and specific behaviours, financial restrictions. At the same time, the social protection's objective is not to create a condition of constant dependency for those in need, but to reintegrate them towards a normal life by encouraging an active lifestyle, increasing the abilities to face problems, reducing the crisis periods by personal efforts mobilization. Concurrently, considering that a healthy person can be integrated more easily and efficiently into the community, the social assistance should focus on guaranteeing at least a minimal protection to fight against medical conditions.

Conclusions

Structural evolutions occurring in modern society generate multiple social risks with a negative influence upon the individuals' security and health, which lead to the increase in the number of socially vulnerable people. Furthermore, social assistance is a state mechanism for social protection through which individuals who became victims due to various factors are offered assistance to recover.

As we have mentioned in the present paper, social assistance is restoring a mutually beneficial interaction between the individuals and the society, having the role to maintain the social balance and the existent social order, to prevent mass disorders or social crisis, or rather, the current situation reveals towards the increase of the social instability. Taking into account the way the pandemic shapes the

process of strategic security development at national and international levels, we consider the area of providing recovery assistance to people who suffered from the SARS-COV-2 consequences should be approached within national policies, not just as an element dedicated to those in need, but as a component of the overall health security.

Approaching the area of social assistance as a structural part of the health security and, respectively, of human security, will determine a greater attention from the state towards this field of great importance for the reintegration of vulnerable individuals into the social community. In this case, the acknowledgment of the social assistance area, as an essential practical dimension in ensuring the citizen's security, is required. Approaching the individual's protection from inter-sectorial perspective is about human security/human health, and social assistance, emphasizes the understanding between the cause and effect of all people's life standard, whatever resources they might have.

References:

1. Agenția Europeană de Mediu (European Environment Agency). (2021). *Mediu și sănătatea.* Available online on https://www.eea.europa.eu/downloads/1c8094f7f3da03a9ac307b70402f2405/1606129147/intro.pdf

2. "CEDO consideră acceptabilă obligativitatea vaccinării". (2021). *DW. Europa*. Available online on https://www.dw.com/ro/cedo-consider%C4%83-acceptabil%C4%83-obligativitatea-vaccin%C4%83rii/a-57135494

3. "Cele mai importante amenințări la adresa sănătății publice, în 2019". (2019). *Ro Health Review Strategies, Economics & More*. Available online on https://rohealthreview.ro/cele-mai-importante-amenintari-la-adresa-sanatatii-publice- in-2019/

4. Comisia Europeana. (2020). *Comunicare a comisiei către parlamentul european, consiliul european, consiliu, comitetul economic și social european și comitetul regiunilor referitoare la Strategia UE privind uniunea securității.* Bruxelles, 24.7.2020 COM (2020) 605 final. Available online on https://ec.europa.eu/ transparency/regdoc/rep/1/2020/RO/COM-2020-605-F1-RO-MAIN-PART-1.PDF

5. Davies, M. (1994). *The Essential Social Worker. An Introduction to Professional Practice in the 1990s*. Ashgate Publishing Limited.

6. Edelstein, Michael, Al. Rafila, F.L. Furtunescu, B.C. Pană. (2021). "Fighting antimicrobial resistance: actions taken across Europe". *European Journal of Public Health*, e-collection AMR. Available online on https://academic.oup.com/eurpub/pages/antimicrobial_resistance

7. Gomez, Oscar A. and Des Gasper. (n.d). *Human Security. A Thematic Guidance Note for Regional and National Human Development Report Teams*. Available online on http://hdr.undp.org/en/content/human-security-guidance-note

8. Hepworth, Dean H., Jo Ann Larsen. (1990). *Direct Social Work Practice: Theory and Skills*. Pacivic grove, C.A: Brooks/Cole, p. 644.

9. *ILO Monitor: COVID-19 and the world of work. Seventh edition Updated estimates and analysis*. (2021). Available online on https://www.ilo.org/wcmsp5/groups/public/-dgreports/dcomm/documents/briefingnote/wcms_767028.pdf

10. Kazmierczak, Aleksandra. (2019). "Cum afectează pericolele de mediu grupurile vulnerabile din Europa. www.eea.europa.eu/re/articles/cum-afectează-pericolele-de-mediu". *Buletin Informativ al Agenției Europene a Mediului*. Available online on https://www.eea.europa.eu/downloads/0dfd6d00c348469e996abae3840b4dc9/1606129115/cum-afecteaza-pericolele-de-mediu.pdf

11. Nate, Silviu. (2014). *Intelligence şi securitate societală. Provocările unei tranziții comune.* București: Editura ANIMV.

12. ONU. (2015). *Declarația universală a drepturilor omului*. Available online on https:// promolex.md/wpcontent/uploads/2018/11/Declaratia-Universala-a-Drepturilor- Omului.pdf

13. *Porto Social Summit*, (May 7, 2021). Available online on https://www.consilium.europa.eu/en/meetings/european-council/2021/05/07/social-summit

14. Proca, Maria, Fortuna, Andrei, Cociug, Svetlana. (2016). "Human Security and the State". *Political science, international relations and security studies*, International Conference Proceedings, the X-th Edition, Sibiu, 450-456.

15. Proca, Maria, Stratan, Valentina. (2020). Riscul social ca factor de legătură între securitatea umană şi asistenta social. *Materialele conferinței ştiințifico-practice naționale. Mandatul de securitate: probleme actuale de interpretare, legislație şi practică,* 118-129.

16. Romanoschi, Florentina, Romanoschi, C. (2012). *Sănătatea populației – altă față a securității***.** București: Editura ANIMV.

17. Stancu, I. (2020). *[România] Eliminarea violenței împotriva copiilor și Covid-19 – Document de poziție Child Rights now.* Available online on https://childhub.org/ro/stiri-protectia-copilului/romania-eliminarea-violentei-impotriva-copiilor-si-covid-19-document-de-pozitie

18. Stratan, Valentina, Proca. Maria. (2020). "Asistența medico-socială – dimensiune practică a securiității sănătății". *Materiale conferinței științifice internaționale Probleme ale științelor socioumanistice și modernizării învățământului,* 239-244, Chișinău.

19. Szabo, Anamaria. (2007). "Construcția socială a conceptului de risc". *Riscuri la tineri. Studiu de caz: adolescenții cu HIV/SIDA în România*. Editura Universității din București, 38-54. Available online on https://www.academia.edu/5745250 Construc%C5%A3ia_social%C4%83

20. UN WOMEN Moldova. (2020). *Analiza impactului Covid – 19 asupra rolurilor de gen*, Chișinău. Available online on https://tandis. odihr.pl/bitstream/20.500. 12389/22645/3/22645_RO.pdf

21. United Nations. (2009). *Human Security in Theory and Practice. Application of the Human Security Concept and the United Nations Trust Fund for Human Security.* Available online on https://www.undp.org/ content dam/turkey/docs/news-from-new-horizons/issue-41/UNDP-TR-HSHandbook_ 2009.pdf

22. *UN Approach to Human Security*. Available online on http://humansecuritycourse.info/module-1-the-concept-of-human-security/ un-approach/

23. Zamfir, E. (20199. *Asistența socială: spațiu de colaborare socio-medicală.* Available online on https://www.romaniasociala.ro/asistenta-sociala-spațiu-de-colaborare- socio-medicala/

24. WHO. (2021). *Weekly Epidemiological and Operational Updates Aprilie 2021*. Available online on http://who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports

INTELLIGENCE IN THE 21ST CENTURY

ANALYSIS OF FRANCE'S NATIONAL ECONOMIC INTELLIGENCE SYSTEM ARHITECTURE

Gabriel-Traian UNGUREANU*

Abstract:

The paper analyses the architecture of the national economic intelligence system of the French Republic, evaluating its degree of compliance in relation with a set of 12 specific characteristics for an efficient economic intelligence system. The analysis is made using the CODV tool of Six-Sigma.

The study validates to what extent France's national security strategy sets out directions to strengthen economic security. At the same time, the article analyses if the architecture of the national economic intelligence system facilitates efforts correlation within the intelligence community and whether the cooperation between the national economic intelligence system's entities categories can be realised. Subsequently, it is analysed whether the economic intelligence system is an integrated component of the national intelligence system, whether it allows all sources analysis and whether it facilitates the use of new technologies through intelligence cycle stages. Following the above steps, it is finally determined with what efficiency the France's economic intelligence system can provide support information needed to increase the competitiveness of the national economy. Thus, analysing areas in which the French economic intelligence system performs, were identified some good practices that can be the basis for proposals to increase the efficiency of the national economic intelligence system.

Keywords: *Economic Intelligence, National Economic Intelligence System, Architecture, Entities, Links, French Republic*.

Introduction

Studying the evolution of economic intelligence systems, referring to the current stage of their development and the stage of economic development of the countries that own them, for an analysis

* PhD student, "Mihai Viteazul" National Intelligence Academy, email: ungureanu.gabriel@animv.eu

that determines sets of best practices, in this paper we chose to study the architecture of the French economic intelligence system. We consider it relevant because France: (1) is a European country that has social, political and institutional environments similar to Romania (Thijs, Hammerschmid & Palaric, 2017, p. 19-67; Uslaner, 2018, p. 359-483; Roper, 2002, p. 256-259; De Meur & Berg-Schlosser, 1994, p. 201-209) and (2) has a well-developed national intelligence system (Pasquazzi, 2017, p. 505; Carayon, 2003, p. 91).

Regarding France's economic system, there are many positive assessments of its incisiveness, omnipresence, and efficiency.[1] Owning an extended economic intelligence apparatus, with a well-consolidated intelligence culture during time, France is recognized and feared in the field of economic intelligence (Reid, 2016, p. 797-799). The quality of the specialized education system, human resources policies, fluency and efficiency of the processes, strong inter-institutional collaboration, good cohesion, and vast social policies (Carayon, 2003, p. 10-13), all developed to support informational demarches, make the French economic intelligence system an important landmark.

The analysis of the French economic intelligence system is based on the consolidated information revealed by Annex 1, which was elaborated using the Literature Analysis, Content and Text Analysis (Walliman, 2011, p. 56-62; MacDonald & Headman, 2008, p. 66-71), Content Analysis of (Open) Web Sources listed in Annex 1.1 (Kim & Kuljis, 2014, p. 285-286; Herring, 2010, p. 237-240), as well as appealing to the specific principles of Social Network Analysis (Wasserman & Faust, 1994, p. 17-21; Olson & Lauhoff, 2019, p. 107-128),

[1] According to: "Espionage? Moi?", https://foreignpolicy.com/2013/07/02/espionage-moi/; "On French Espionage", https://www.lawfareblog.com/french-espionage; "Robert Gates: Most Countries Conduct Economic Espionage", https://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/; "WikiLeaks: France Leads Russia, China in Industrial Spying in Europe", https://www.cbsnews.com/news/wikileaks-france-leads-russia-china-in-industrial-spying-in-europe/; "France is top industrial espionage offender", https://www.france24.com/en/20110104-france-industrial-espionage-economy-germany-russia-china-business; "The French economic intelligence and the Intelco case", https://moderndiplomacy.eu/2018/03/28/the-french-economic-intelligence-and-the-intelco-case/, accessed on 20-08-2021.

applied according to Multiple Relations Model (Wasserman & Faust, 1994, p. 73-77; Carayon, 2003, p. 91-115) and Nondirectional and Directional Relations Model (Wasserman & Faust, 1994, p. 223-230; MacArthur, 1994, p. 234).

Annex 1 list the entities with an economic, intelligence or mixed role related to the French National Economic Intelligence System. The direct relationships (direct subordination within the same group of entities) are highlighted with continuous lines, and the indirect ones (no direct subordination, functional, consultative roles) with dashed lines (Carayon, 2003, p. 112). The architecture highlights the entities, grouped in four distinctly illustrated categories: the Administrative Apparatus, the Diplomatic Apparatus, the Intelligence Services, and the Business Environment. Within the analytical approach, the reporting to the role of entities is done as follows: entities with a single role; intelligence, entities with a mixed role; intelligence and economic intelligence, entities with a single role; economic intelligence. Regarding the type of relations between entities, they are categorized as follows: indirect relationship between economic intelligence entities, direct relationship between economic intelligence entities, indirect relationship between intelligence services, and direct relationship between intelligence services (Wasserman & Faust, 1994, p. 224; Arboit, 2016, p. 27).

Subsequently, by reporting to the Conceptual Framework Analysis (Jabareen, 2009, p. 52-55; Lederman & Lederman, 2015, p. 593-597), it was determined that the French economic intelligence system compliance score depends on 12 **critical characteristics**[2] (marked below with [**6σ C**]), specific to an efficient economic intelligence system. The analysis was performed using the Six-Sigma[3] – CDOV tool, giving

[2] Those 12 characteristics were determined by the author and validated by local experts through a research which used the Delphi method, from September 2019 till March 2020. More details can be found in the author's paper "Evolutions, trends and essential characteristics of economic intelligence systems", Scientific Report, Library of "Mihai Viteazul" National Intelligence Academy, Bucharest, 2020.

[3] According to: Cutcher-Gershenfeld, J., "Lean/ Six Sigma Processes"; Murman, E. "Introduction to Lean Six Sigma Methods. Lecture Notes" and Pyzdek, T. "The Six Sigma Handbook".

for each characteristic a score from one (very low) to five (very high)[4] for compliance degree, resulting a maximum score of 60.

Analysis of the French Republic's economic intelligence system architecture

1 | [6σ C] Qualitatively analysing the national security strategy, to what extent does it include strategic lines regarding the development and consolidation of sectors specific to economic intelligence?

[**6σ D**] In the preamble of the French Republic's security strategy there are two main issues underlying the strategy base: France cannot address alone all challenges and France has global economic interests and interests regarding the access to new technologies, to flows of goods and human resources?

The strategy is structured into three parts. In Part A – "*A Rapid and Lasting Deterioration of the Strategic Environment*" it is pointed out that the rivalry, initially economic and technological, is increasingly present in the military area. Part B – "*New Forms of Warfare and Conflict*", emphasizes the need to secure land, sea, and air routes, in order to carry out the economic operations (French Presidency, 2017, p. 43-44). In Part C – "*Our Defence Strategy - Strategic Autonomy and European Ambition*", the emphasis is on "*Defence Industrial and Technological Base*"[5] (DITB), which supports the national economy and extends France's international influence. The technological superiority

[4] In order to have a consistent analytical framework, for each critical characteristic, five analytical questions were elaborated, verifying the economic intelligence system capacity to comply with each characteristic. More details can be found in the author's paper "Comparative Analysis of the United States of America and France National Economic Intelligence Systems", Scientific Report, Library of "Mihai Viteazul" National Intelligence Academy, Bucharest, 2021. The scoring of each analytical question/ characteristic was done by the author. To achieve accurate scores, in the near future we intend to carry out a Delphi study which will address representative experts.

[5] DITB (France's Defence Industrial and Technological Base) consists of 12 global corporations and around 4,000 small and medium-sized companies. Most of them use cutting edge technologies and have a major positive impact on France's trade balance.

and strategic autonomy of France depend on sustainability and performance of the DITB's entities (French Presidency, 2017, p. 63-72).

In addition, all sections of the strategy include elements that emphasize the need to develop economic intelligence and to protect key economic entities, but those are not focused to ensure the security of most economic actors and there are no mentions regarding concerns around the well-being of the population. Strategic autonomy remains the key objective of security policy. In this context, strengthening the DITB is a priority (French Presidency, 2017, p. 63-67). Diplomacy is seen as an inseparable component of defence, both requiring close coordination with "*civilian instruments*": Business Environment and Administrative Apparatus (French Presidency, 2017, p. 54-73).

At the same time, the defence strategy mentions that "*friction and confrontation are no longer restricted to disputed geographical areas, but now involve the digital domain as well*" (French Presidency, 2017, p. 13), becoming, "*subject of intense strategic competition*" (French Presidency, 2017, p. 45). Therefore, because cyberspace makes the usual distinction between peace, crisis, and war unclear, France has decided to adopt "*a permanent cybersecurity posture*", achieving a substantial increase of specific capabilities, in order to engage specific defensive or offensive operations in the digital (French Presidency, 2017, p. 47-90).

[**6σ O**] In conclusion, the economic component is a transversal one in the 2017 macro-strategy, without having a central position in France's security strategy. France treats economic issues in a general note, excepting DITB, the French state providing support for all DITB economic entities (French Presidency, 2017, p. 63-64). Without being approached from an economic intelligence perspective, new technologies and cybersecurity are considered critical.

[**6σ V**] Thereby for Question one, on a scale from one to five, given that strategic measures are envisaged, but are not framed in an economic picture, three is the value which describes how the national security strategy meets the needs of economic intelligence.

2 | [6σ C] Analysing the structures of the national intelligence system and the national economic intelligence, how do you appreciate that the economic intelligence system is integrated into the national intelligence system architecture?

[6σ D] Analysing the overlaps between the national intelligence system and the national economic intelligence system, as presented in "*Annex 1 – National Intelligence System and National Economic Intelligence System of France*", we noticed that out of a total of 60 entities, 39 have an exclusive role within the national economic intelligence system, 11 have an exclusive role within the national intelligence system and another 10 entities have a mixed role.

Both from defensive and offensive perspectives, the information collected from the Business Environment by entities from key ministries of the economic intelligence system (Ministry of Higher Education, Research and Innovation, Ministry of Economy and Finance, and Ministry of Europe, Foreign Affairs and the Diplomatic Apparatus) are consolidated at the level of the Prime Minister and of the Government Information Service (SIG). Information which is delivered by Intelligence Services is consolidated at the level of the General Secretariat for Defence and National Security (SGDSN)/ Defence and National Security Council (CDSN) and the President of the French Republic.

Integration between the categories of entities is made at the level of the President where the connection between Intelligence Services, Administrative Apparatus, Diplomatic Apparatus, and Business Environment entities is made through the SIG, the CDSN and advisory entities: Council of Economic Analysis (CAE), Centre for Research and Expertise on the World Economy (CEPII) and the Economic, Social and Environmental Council (ESEC). At the same time, integration of intelligence delivered by the Administrative Apparatus, the Diplomatic Apparatus and the Intelligence Services is realized at the level of the Prime Minister, through direct communication channels.

[6σ O] Relating (quantitatively) strictly to the number of entities, there is a 47.6% overlap.[6] The information that supports the

[6] The percentage resulted from the ratio between the number of entities with a mixed role (intelligence and economic intelligence) and the number of entities that are part of the national intelligence system (Annex 1.2 – "Entities and Relationships").

offensive and defensive economic roles is centralized at the President, SIG and CDSN levels. This fact gives the advantage of an integrated vision but may have the disadvantage of a lack of specialization.

[**6σ V**] In conclusion, we consider that a score of four best describes the degree of national economic intelligence system integration into the national intelligence architecture.

3 | [6σ C] Analysing the national intelligence system structure and the national economic intelligence system structure, on a scale from one to five, what do you consider to be the offensive orientation of the national economic intelligence system?

[**6σ D**] Analysing Annex 1, we notice that DGSE (including the Economic Security Division) and the Directorate General for International Relations and Strategy (DGRIS) have an active role in collecting economic information and conducting external operations to support distinct economic initiatives. The CDSN ÷ SGDSN tandem and the SIG also play an active support role. The Diplomatic Apparatus and the National Intelligence and Counter-Terrorism Coordination (CNRLT) could provide tactical support.

The Administrative Apparatus integrates, consolidates, and provides information for the Business Environment through specialized portals such as service-public.fr, legifrance.gouv.fr, data.gouv.fr. At the same time, Business France, BPI France, and the Diplomatic Apparatus, seconded by the Chambers of Commerce and Industry (CCI) and private companies such as AFNOR Group, ADIT Group or COFACE, collect, integrate, correlate, and deliver information to the Business Environment, supporting in an active manner the business actors. Other entities that collect and process information intended to support external economic operators are CNSR – INIST, CSR, ESEC, CEPII and CAE. Both BPI France and the CCI have direct links with the Business Environment. The CCI is actively involved, provides support to external economic entities, and ensures their connection with the Administrative Apparatus. Situationally, the Diplomatic Apparatus can also support certain economic entities of the Business Environment, at the same time being the vehicle (vector) through which the Intelligence Services could provide support to the economic entities, the French

intelligence community not having direct channels of communication with the Business Environment.

[**6σ O**] In conclusion, only situationally, the external intelligence system and the Diplomatic Apparatus can play an active role in the national economic intelligence system. The Administrative Apparatus, integrated in the national economic intelligence system's architecture, is able to take offensive roles.

[**6σ V**] Thereby, for question three, we consider that four is the value that describes the offensive orientation of the national economic intelligence system, taking into consideration the fact that there are no direct lines of communication between the Diplomatic Apparatus, Intelligence Services, and the Business Environment.

4 | [6σ C] Analysing the structure of the national intelligence system and of the national economic intelligence system, on a scale from 1 to 5, what do you consider to be the defensive orientation of the national economic intelligence system?

[**6σ D**] There are entities within the Administrative Apparatus[7] that can collect economic information and disseminate it at the level of the SIG, Prime Minister, CDSN, and President of the French Republic. DGSI, DRSD and DGRIS have an active role to play in collecting economic information and conducting internal operations, designed to support certain economic initiatives. The CDSN ÷ SGDSN tandem and the SIG have an active role, and the DGSI and the CNRLT have the capacity to provide tactical support for certain economic actors of Business Environment. Situationally, the Ministry of Economy and Finance can also join. At the same time, data.gouv.fr, service-public.fr

[7] The Ministry of Economy and Finance through the National Directorate of Customs Information and Investigations (DNRED), the Directorate for Information Processing and Action against Illegal Financial Circuits (TRACFIN) and the General Directorate of Social Cohesion collect and disseminate economic information. Other entities that collect and process information meant to support the internal economy are the Institute of Scientific and Technical Information (CNSR - INIST) and the Strategic Research Council (C.S.R) within the Ministry of Higher Education, Research and Innovation and the Economic, Social and Environmental Council, Centre for Research and Expertise on the World Economy (CEPII) and the Council of Economic Analysis (CAE) assisting the French Presidency and the Prime Minister.

and legifrance.gouv.fr have the role of integrating and consolidating the information mainly from the area of the Administrative Apparatus, then some sets of information from Diplomatic Apparatus and the Intelligence Services and of making them reachable for Business Environment. Both from offensive and defensive perspectives, the CCI has the capacity to communicate directly and provide support to all entities of the Business Environment engaged in internal or external activities. At the same time, the CCI has the capacity to connect the Business Environment with the Administrative Apparatus. This creates channels through which the SIG, CDSN/ SGDSN can situationally provide support to the Business Environment, being also a vehicle for the French Intelligence Services.

[**6σ O**] In conclusion, France's national internal intelligence system has an active role, collecting and disseminating economic intelligence, the internal public and the Administrative Apparatus having the capacity to play an active role. There are channels through which economic information can be collected and disseminated to and from internal Business Environment and there are available mechanisms through which the economic intelligence system entities are able to provide support and ensure the security of economic operations.

[**6σ V**] We can appreciate that for the fourth question, four is the value that describes the defensive orientation of the national economic intelligence system, considering that, regarding the existence of direct communication channels between the Intelligence Services, the Diplomatic Apparatus, and the Business Environment, and those are not at a full scale.

5 | [**6σ C**] **Analysing the architecture of the national economic intelligence system, referring strictly to the relations between the Administrative Apparatus, Business Environment, Diplomatic Apparatus, and Intelligence Services, from a structural point of view, is there a possibility of effective collaboration, synchronization of efforts and mutual support between all sectors?**

[**6σ D**] The connections between the Intelligence Services and the Business Environment that make up the Business Environment are made through two routes: offensive ÷ external (Intelligence Services

(DGSE) ÷ CNRLT / CDSN ÷ French Diplomacy / Ministry of Europe and Foreign Affairs ÷ Business Environment) and defensive ÷ internal (Intelligence Services (DGSI) ÷ SIG ÷ Ministry of Higher Education, Research and Innovation / Ministry for Economy and Finance ÷ Business Environment). The system's architecture ensures indirect communication between the Diplomatic Apparatus and the Business Environment. At the same time, there is another channel: the Diplomatic Apparatus ÷ Ministry of Europe and Foreign Affairs ÷ CCI ÷ Business Environment. Other intermediaries, similar to CCI, may be the private companies specialized in business and competitive intelligence (ANFOR, COFACE, ADIT), consulting companies or investment funds. Through the CCI, the system's architecture allows direct communication between the Administrative Apparatus and the Business Environment.

[**6σ O**] In conclusion, there are communication channels, areas of interference between Intelligence Services, the Diplomatic Apparatus, and the Administrative Apparatus, but there is no direct institutional communication between the Intelligence Services and the Business Environment (Arboit, 2016, p. 27-28). The system's architecture provides communication channels between the Diplomatic Apparatus, the Administrative Apparatus, and entities of the Business Environment.

[**6σ V**] For question five we give the score four, because the system architecture does not provide direct communication between Intelligence Services and the Business Environment.

6 | [6σ C] Analysing the national economic intelligence system structure, strictly referring to the relations between the Administrative Apparatus, the Business Environment, the Diplomatic Apparatus, and the Intelligence Services, can we consider that the economic organizations involved in international trade are supported?

[**6σ D**] Business community can directly receive support and assistance from CCI. At the same time, situationally, the Ministry for Europe and Foreign Affairs through its directorates is also able to support business community. The Diplomatic Apparatus can provide

indirect support to the Business Environment. The SIG connects the Intelligence Services with the Administrative Apparatus.

[**6σ O**] The conclusion is that the architecture of the economic intelligence system allows, in a situational manner, the Administrative Apparatus and the Diplomatic Apparatus to provide support to entities of the Business Environment engaged in international trade.

[**6σ V**] For question six, we set a score of three points, because the economic intelligence system architecture allows the Intelligence Services, the Administrative Apparatus, and the Diplomatic Apparatus to directly support economic to entities of the Business Environment involved in international trade, only in certain situations.

7 | [**6σ C**] **Structurally, is it possible to set and calibrate direct communication between entities. Moreover, can the structure of the economic intelligence system allow strict procedures implementation?**

[**6σ D**] The architecture of the French national economic intelligence system meets the basic requirement for the implementation of a platform that ensures efficient real time communication, respects the information security requirements, and facilitates information management. Thereby, between the Administrative Apparatus entities and the Business Environment there is a direct, two-way communication through the CCI. At the same time, between Diplomatic Apparatus and the Business Environment direct channels can be implemented, with the Ministry of Europe and Foreign Affairs as a vector. Also, the system structure allows direct communication between the Intelligence Services and the Diplomatic Apparatus. Regarding the communication between the Intelligence Services and the Administrative Apparatus, it can be realised through SIG. Intelligence Services do not directly communicate with the Business Environment, those only collect information.

[**6σ O**] In conclusion, structurally, it may be possible to calibrate the communication between entities. The structure of the economic intelligence system partially allows the implementation of strict procedures for three of the five possible communication channels.

[**6σ V**] Consequently, for question seven the score is three.

8 | [6σ C] Does the system structure allow the adoption and use of the new technologies to facilitate collection from multiple sources, efficient processing, and dissemination of information between Intelligence Services and other entities of the system?

[**6σ D**] From the analysis of the flows outlined in Annex 1, we find that the architecture of the system allows the continuous and structured data collection from the Diplomatic and Administrative Apparatuses, as well as from the Business Environment. Both, collection, and information processing, can be done technologically. However, with regard to the information dissemination to certain Business Environment entities, excepting CCI, no other direct communication channels have been identified.

[**6σ O**] The system architecture allows adoption and use of new technologies to facilitate multiple sources collection and efficient information dissemination between Intelligence Services and other entities.

[**6σ V**] Consequently, for question eight, we consider that five points can be awarded.

9 | [6σ C] Does the structure of the system allow the Diplomatic Apparatus to systematically collect economic and strategic information from the Business Environment?

[**6σ D**] From the analysis of Annex 1, we notice that the Diplomatic Apparatus plays a situational role in the Business Environment, thereby, it can collect information punctually, but not in a continuous and systematic manner. Consequently, it is unlikely to collect and aggregate strategic information in an efficient manner. This category of information may be systematically collected by other entities, such as CCI, BPI France, or other entities within the Administrative Apparatus, thus respecting centralization tendency of the French EI system.

[**6σ O**] The structure of the system allows the Diplomatic Apparatus to situationally collect mainly tactical economic information from Business Environment.

[**6σ V**] Indirect communication channels are set mainly between the Intelligence Services and the other categories of entities. Consequently, we award three points for question nine.

10 | [6σ C] Can system architecture facilitate all sources analyses and integrate in the analytical approach types of information, other than those from Diplomatic Apparatus and Intelligence Services, as multiple sources databases, private sources, and other information collected from non-intelligence sources?

[**6σ D**] Analysing the French IE system's entities and their relationships, we see that Intelligence Services can collect, mainly through indirect channels, domestic business information, foreign business information, as well as information from local and foreign professional databases.

[**6σ O**] Intelligence Services can build through functional communication channels a unique database that integrates all types and categories of sources.

[**6σ V**] Thereby, for question 10 the score is three, given that at least two layers of entities are interposed between the Intelligence Services and the Business Environment, which can make extended collection and all sources' analyses difficult.

11 | [6σ C] Internally, does the architecture of the economic intelligence system allow for the monitoring of all key areas?

[**6σ D**] Information from academia and research institutes is monitored and consolidated at the SIG level, with a direct line of communication between areas. In the same way, the political and legal information is consolidated at the SIG and CDSN levels. The Intelligence Services actively monitor media and social media, the information being consolidated at the level of the CNRLT. However, in terms of strengthening domestic and foreign economic information, the tandem DGSE ÷ Department of Economic Security and Department of Cyber Security within DRSD, which can allow effective monitoring and an increased response capacity.

[**6σ O**] In conclusion, the national economic intelligence system structure allows for the monitoring of the main key areas, but functional communication channels affect the agility of the system.

[**6σ V**] We note that the system architecture allows monitoring of most key areas; consequently, for question 11 the score is four.

12 | [6σ C] Structurally, can people and private overseas investments be properly protected?

[**6σ D**] The tandem of DGSE ÷ the Department of Economic Security and the Department of Cyber Security within DRSD, can successfully monitor and detect threats to external assets and key personnel operating outside French territories. The same structure can monitor key people and entities that can influence the overseas competitive Business Environment. At the same time, at the level of the CNRLT or the SIG, involving the Diplomatic Apparatus, the necessary countermeasures can be drawn up and implemented to counteract these types of threats. Regarding the macro-environment monitoring, it can be done by the specific ministerial directions, the information being consolidated at the level of the SIG.

[**6σ O**] In conclusion, the system architecture allows the monitoring of threats to assets and key personnel operating abroad, with some shortcomings related to the operationalization of countermeasures.

[**6σ V**] For question 12, the score is four, as there are levers through which people and private investments overseas can be protected.

Conclusion regarding the French National Economic Intelligence System

Following the analysis of the French national economic intelligence system architecture, centralizing the above conclusions, referring to the system's efficiency from a structural point of view, we get an aggregate score of 44 points out of a maximum of 60, which results in a yield of 73.3% (out of 100%):

	the critical characteristics of France's national intelligence economic system	Maximal Score	France's Score
		60	44
1	national defence strategy contain lines regarding economic security	5	3
2	national E.I. system should be embedded into the national intelligence one	5	4
3	the national E.I. system should adopt the offensive roles	5	4
4	the national E.I. system should adopt the defensive roles	5	4
5	efficient cooperation between intelligence ÷ administration ÷ diplomacy ÷ busine	5	4
6	E.I. system entities support the economic organizations and the international trad	5	3
7	fast and easy communication between the all categories of entities	5	3
8	adoption and use of new technologies in all stages of intelligence cycle	5	**5**
9	diplomacy collect and disseminate economic and strategic information	5	3
10	all sources analysis is essential in the E.I. processes	5	3
11	monitoring of all key intelligence areas is essential in the E.I. processes	5	**4**
12	E.I. system entities protect people and private investments from abroad.	5	4

Figure 1: Aggregate score of the French national economic intelligence system architecture analysis (authors' idea)

The French economic intelligence system is integrated into the intelligence ecosystem, being a mature system, with proven results and sets of good practices consolidated over time (ieee, 2003, p. 18-19). It is a complex system that operates on a global scale, with an increased focus on the French territories[8] (ieee, 2003, p. 21-22). The intelligence integration and consolidation is mainly performed at the level of the Prime Minister ÷ Presidency (with specific adjacent entities), which creates a certain "*bureaucratization*" of communication and partially affects the agility of the system (Arboit, 2016, p. 26-29; Denece, 2020, p.5). However, we are dealing with one of the most efficient economic intelligence systems in the world (Pasquazzi, 2017, p. 506) which stands out by:

- a good segmentation of expertise. The expertise is consolidated at the level of each ministry through specific organizations, structures and substructures (ieee, 2003, p. 54). For example, at the Ministry for Europe and Foreign Affairs level we have AFD, CFI, CIRAD, IRD, Business France, France Media Monde but also BPI.

[8] We refer to: Guadeloupe, French Guiana, Martinique, Réunion, Mayotte, but also to French Polynesia, Saint Pierre and Miquelon, Wallis and Futuna, Saint Martin, Saint Barthelemy, New Caledonia or the French southern and Antarctic territories.

Inter-ministerial consolidation takes place at the level of CEPII, ESEC and CAE, supporting the Presidency and the Prime Minister. The aggregation of all information (but also of knowledge and expertise) is made at the level of the SIG that communicates directly with SGDN ÷ CDSN.[9]

- **a good correlation and efforts concentration to deal with strategic situations** that may have a negative impact at national or DITB levels. Consolidations are made at the Prime Minister level, integrating all data collected by the SIG, SGDN ÷ CDSN, the Ministry of Armed Forces, the Ministry of Interior and the CNRLT. Thus, a comprehensive image is provided, with information from all areas of interest. At the same time, concerning risk situations or strategic issues, all available levers can be addressed, and all available resources engaged, allowing firm and efficient countermeasures (Gagliano, 2016, p. 5). France is now trying to transfer these practices and disseminate expertise at European level. In September 2017, President Emmanuel Macron suggested a European Intervention Initiative (EI2) as part of his vision of a "sovereign Europe united and democratic" (Zandee & Kruijver, 2019, p.1). Some voices have labelled the proposal as the launch of a European intervention force. EI2 aims to bring together capable and willing European countries to better prepare for future crises - not by creating a new passive reaction force, but by ultimately creating a common pro-active strategic culture. Ten European countries have joined France's initiative (Zandee & Kruijver, 2019, p. 1-4).

- **an academic system that created precise specializations for most professionals, allowed clear expertise segmentation, and formed extensive global networks of specialists.** We are referring to a complex system, built over time, which allows a good specialization, the consolidation of knowledge specific to a certain segment and the efficient transmission of information between generations of professionals, necessary to ensure continuity (Pasquazzi, 2017, p. 513-154). We mention here the National School of Administration, the National Institute of Higher Security and Justice Studies (INHESJ), Institute of Highers National Defence Studies (IHEDN), the Intelligence

[9] Please see "Le Conseil de défense et de sécurité nationale", at: https://www.elysee.fr/la-presidence/le-conseil-de-defense-et-de-securite-nationale, last accessed on 21st of Augus 2021.

Academy and School of Economic Warfare (EGE) (Harbulot, 2021, p. 52-55). For example, it is extremely difficult to identify, in a management position in the Administrative Apparatus, a person who has not attended the courses of the National School of Administration. In this academic system, EGE ("*Ecole de Guerre Economique*") has a special role (Gagliano, 2016, p. 7). Created in 1997 at the recommendation of the Economic Intelligence Commission, this is the place where the executives of French strategic interest companies are currently prepared (Harbulot, 2021, p. 52-53). With the passage of time, this network has been extended at an international scale. Moreover, with a diversified program adapted to the current context, in the last 25 years it has been turned into a network with more than 2,000 economic intelligence experts, key people holding executive positions in strategic companies spread all over the globe. EGE's alumni network comprise over 30 clubs, grouped by territories (eg "Club Russie", "Club Suisse", "Club Asia") and areas of interest (eg "Club Start-up & Innovation", "Club Data Intelligence", "Club Analyze").[10]

- ***an academic system that has created a genuine security culture throughout society.*** *Worth noticing is the project initiated in 2003 by Bernard Carayon (with the "Carayon Report"). The project aimed to strengthen the culture of (economic) security at all levels of society and to achieve social cohesion. This approach has continued over the years and has been directly reflected in public policies (Gagliano, 2018, p. 1-3). Today, within the Ministry of Economy and Finance, there is the General Directorate of Social Cohesion that elaborates specific strategies and follows their implementation and efficiency (Pasquazzi, 2017, p. 508).*

The French economic intelligence system is characterized by efficient and vigorous actions, performed in a firm manner. They are possible through a good mobilization of forces by the coordinating and commanding entities around the president ÷ prime-minister tandem. Command and coordination cluster is focused mainly on strategic actions, aiming to support strategic companies and DITB entities, other economic operators being out of its scopes (Tarlogic, 2019, p. 1-3). At the same time, specialization and consolidation of knowledge specific to

[10] Please see "ALUMNI EGE", at: https://www.aege.fr/, last accessed on 21st of August 2021.

a certain segment at the level of each ministry (and academic institutions) ensures continuous progress and efficient transmission of information between generations of professionals, but, in the case of complex actions involving knowledge and specialists from different areas, the coordination and command entities also have the role of bringing together diverse expertise (Harbulot, 2021, p. 52-55).

Continuous efforts to achieve and strengthen social cohesion have allowed both a good collection, from multiple sources and an efficient dissemination of information, most economic entities being thus involved and responsible. At the same time, the formation of a security culture down to the level of each economic operator has created over time a certain "*collective immunity*" (Gagliano, 2016, p. 5). Even if the French economic intelligence system does not aim to protect or directly support economic agents, each economic entity can decide and operationalize its own measures of a defensive or offensive nature, in this context the role of the EGE being even better defined. Attempts were thus made to compensate for the lack of agility by transferring knowledge to most economic operators (Gagliano, 2018, p. 1-3).

In conclusion, France's economic intelligence system allows the adoption of new technologies at the level of entities specific to the Administrative Apparatus, the Diplomatic Apparatus, and the Intelligence Services (Gagliano, 2017, p. 49680). At the same time, being a centralized system, controlled from the level of the president and the prime minister, for sensitive strategic topics, integration and all required correlations with the Intelligence Services are easily ensured. Regardless of the nature of the operations, offensive or defensive, the economic intelligence system allows the efficient addressing of situations with strategic impact, subscribed to the national interest. At the same time, the creation of a central command structure facilitates good monitoring of key economic areas (Tarlogic, 2019, p. 1-3).

All these are possible because the national security strategy reflects economic intelligence as a necessity for the protection of DITB and strategic economic entities and, consequently, these directives are transposed into Intelligence Services missions (Gagliano, 2017, p. 49682). The national economic intelligence system entities have well-defined roles and clearly outlined objectives, information

superstructures that facilitate communication being created and, at the same time, ensuring the consolidation of strategic information (Tarlogic, 2019, p. 1-3). Also, there is a specialization of entities, as there are clusters of experts, as the level of ministries, which facilitate expertise consolidation and ensure a good knowledge transfer between generations of professionals. At the same time, cross-cutting projects related to research, development, and implementation of cutting-edge technologies in the field of defence and security are supported (Pasquazzi, 2017, p. 513-154). The academic system supports in a concerted manner the development of economic intelligence by facilitating the creation of extensive professional networks and a true culture of intelligence throughout society and French Administrative Apparatus implements public policies and coherent programs to achieve good social cohesion and to form a veritable security culture down to the level of each economic entity (ieee, 2003, p. 56-57).

Conclusions of the work

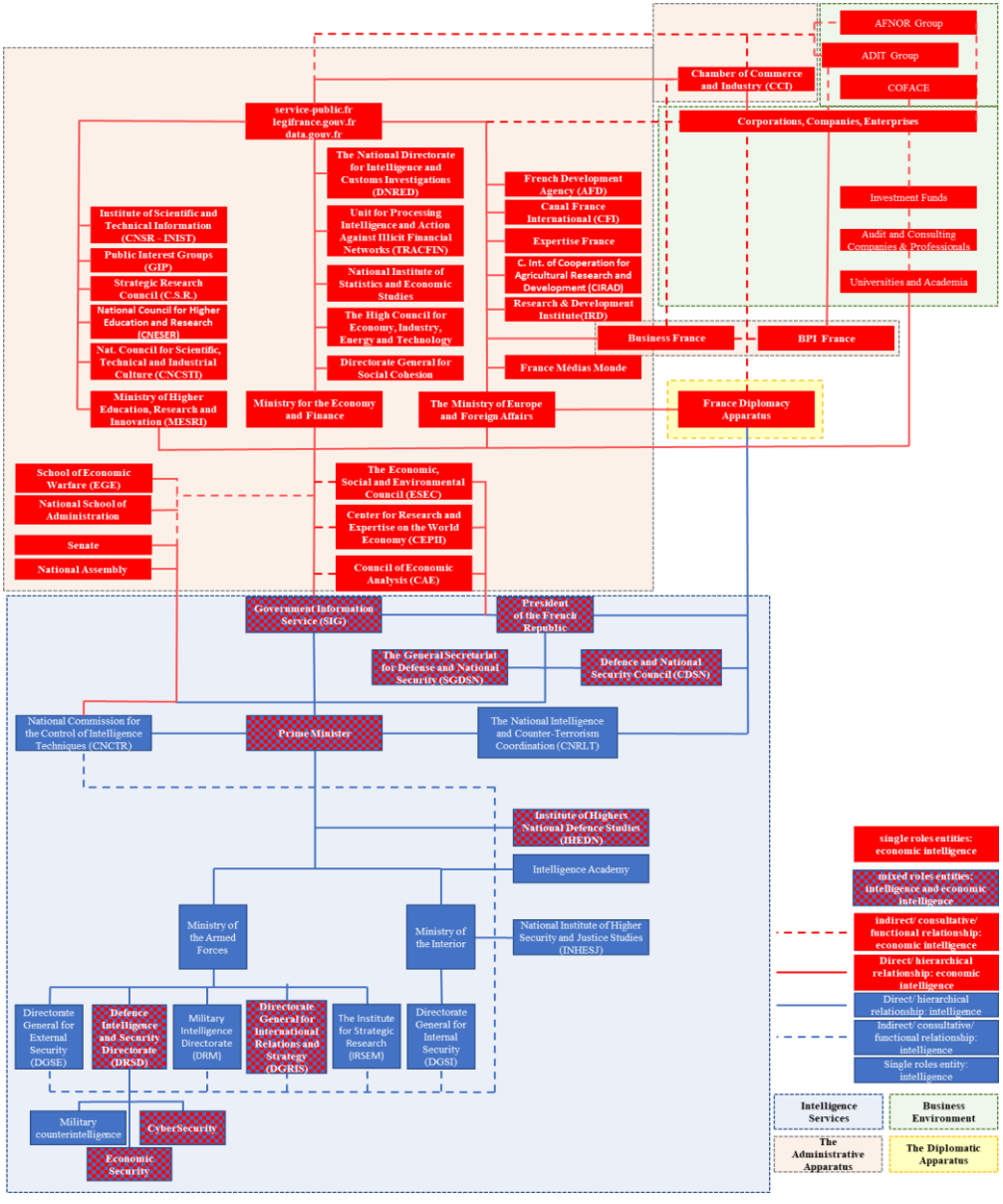
The paper determined the following set of good practices of the French economic intelligence system, as follows:

- economic intelligence is reflected as a need in the national security strategy and, as a consequence, those strategic directives are transposed into missions of Intelligence Services;
- the national economic intelligence system entities have well-defined roles and their objectives are clearly set;
- intelligence superstructures are created to facilitate communication, while also facilitate the consolidation of strategic intelligence;
- there is a specialization of the entities, as there are clusters of experts at the level of the ministries, which allows expertise consolidation and ensures a good transfer of it between the generations of specialists;
- cross-cutting projects related to research, development and implementation of cutting-edge technologies in the field of defence and security are priority supported;
- the academic system supports, in a concerted manner, the development of economic intelligence by facilitating the creation of

extensive professional networks and a true culture of intelligence throughout society;

- coherent public policies and programs are implemented in order to achieve a good social cohesion and to form a true culture of security down to the level of each economic entity.

Annex
National Intelligence System and National Economic Intelligence System of France Entities and Relationships



The architecture of the French national economic intelligence system from Annex 1.2 was elaborated based on the following list of entities and web references, latest accessed on 20th of August, 2021:

- http://www.cae-eco.fr/Presentation-in-english
- https://www.lecese.fr/en
- http://www.cepii.fr/CEPII/fr/welcome.asp
- http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-secretariat-pour-le-conseil-de-defense-et-de-securite-nationale/
- https://www.elysee.fr/
- https://www.gouvernement.fr/ministre/jean-castex
- https://www.gouvernement.fr/secretariat-general-pour-l-investissement-sgpi
- https://www.conseil-national-industrie.gouv.fr/
- https://www.gouvernement.fr/en/everything-you-should-know-about-the-saip-public-alert-mobile-app
- https://forum.wordreference.com/threads/sig-service-dinformation-du-gouvernement.2947974/
- https://www.atinternet.com/en/resources/resources/french-governement-information-service-sig/
- https://www.elysee.fr/cnrlt
- https://www.senat.fr/
- https://www.assemblee-nationale.fr/
- https://www.cnctr.fr/
- https://www.interieur.gouv.fr/Le-ministere/DGSI
- https://www.defense.gouv.fr/ministre
- https://www.defense.gouv.fr/dgse
- https://www.drsd.defense.gouv.fr/
- https://www.defense.gouv.fr/ema/directions-services/direction-du-renseignement-militaire/la-drm
- https://www.defense.gouv.fr/dgris
- https://www.irsem.fr/
- https://www.economie.gouv.fr/ministeres#
- https://www.economie.gouv.fr/ministeres#popin-120796
- https://www.economie.gouv.fr/ministeres#popin-38864
- https://www.insee.fr/fr/accueil
- https://www.economie.gouv.fr/tracfin

- https://www.douane.gouv.fr/fiche/la-direction-nationale-du-renseignement-et-des-enquetes-douanieres
- https://www.enseignementsup-recherche.gouv.fr/
- https://www.enseignementsup-recherche.gouv.fr/cid134437/le-conseil-national-culture-scientifique-technique-industrielle.html
- https://www.enseignementsup-recherche.gouv.fr/cid53497/le-conseil-national-de-l-enseignement-superieur-et-de-la-recherche-c.n.e.s.e.r.html
- https://www.enseignementsup-recherche.gouv.fr/pid25366/acces-thematique.html?theme=369&subtheme=370
- https://www.inist.fr/
- http://www.cnrs.fr/fr
- https://www.gouvernement.fr/ministere-de-l-europe-et-des-affaires-etrangeres
- https://www.francemediasmonde.com/ro/
- https://www.businessfrance.fr/
- https://www.bpifrance.fr/
- https://www.ird.fr/
- https://www.cirad.fr/accueil
- https://www.expertisefrance.fr/web/guest/accueil
- https://cfi.fr/fr
- https://www.afd.fr/fr
- https://www.diplomatie.gouv.fr/en/the-ministry-and-its-network/maedi-21-global-diplomacy-for-the-21st-century/
- https://www.ege.fr/index.php/l-ecole.html
- https://www.ena.fr/eng/
- https://www.ihedn.fr/
- http://www.academie-renseignement.gouv.fr/
- https://inhesj.fr/
- https://www.cci.fr/web/portail-acfci/accueil
- https://www.adit.fr/
- https://www.afnor.org/
- https://www.coface.fr/

References:

1. Arboit, G. (2016). "Une Brève Histoire Contemporaine du Renseignement Français". *Hermes.* 76(3), p. 26-30.

2. Carayon, B. (2003). "Economic Intelligence, Competitiveness and Social Cohesion". *Report to the Prime Minister Jean-Pierre Raffarin*. Government of France, Paris.

3. Cutcher-Gershenfeld, J. (2004). "Lean/ Six Sigma Processes", *MIT Open Courseware*. Available on https://ocw.mit.edu/courses/engineering-systems-division/ esd-60-lean-six-sigma-processes-summer-2004/lecture-notes/ (Accessed August 20, 2021).

4. De Meur, G. Berg-Schlosser, D. (1994), "Comparing political systems: Establishing similarities and dissimilarities", *European Journal of Political Research*, 26(1), p. 193-219.

5. Denece, E. (2020), "L'Intelligence Economica e le Spionaggio", *Conferenza ALL'IASSP, Milano, 29th of November 2020.* Available on https://cf2r.org/ reflexion/lintelligence-economica-e-le-spionaggio-conferenza-alliassp-milano-29-novembre-2019/ (Accessed August 20, 2021).

6. Gagliano, G. (2016), "Guerre Économique et Guerre Cognitive". *Tribune Libre 64(6).* Available on https://cf2r.org/tribune/guerre-economique-et-guerre-cognitive/ (Accessed August 21, 2021).

7. Gagliano, G. (2017), "The Economic Intelligence in France". *International Journal of Current Research 9(4).* Available on https:// www.journalcra.com/ sites/default/files/issue-pdf/22065.pdf (Accessed August 21, 2021).

8. Gagliano, G. (2018), "The French economic intelligence and the Intelco case". *Modern Diplomacy.* Available on https://moderndiplomacy. eu/2018/03/28/ the-french-economic-intelligence-and-the-intelco-case/ (Accessed August 20, 2021).

9. Goffman, E. (1986), "Frame Analysis: An Essay on the Organization of Experience". Northeastern University Press.

10. Goldsmith, J. (2013). "On French Espionage", *Lawfare Blog*, Available on https://www.lawfareblog.com/french-espionage (Accessed August 20, 2021).

11. Harbulot, C. (2021). "L'École de guerre économique: une success story française", *Constructif*. 58(1). P. 52-55.

12. Herring, S.C. (2010). "Web Content Analysis: Expanding the Paradigm", *International Handbook of Internet Research*. Springer. New York. p. 233-249.

13. Jabareen. Y. (2009). "Building a Conceptual Framework: Philosophy, Definitions, and Procedure", *International Journal of Qualitative Methods*, 8(4). p. 49-62.

14. Keck, Z. (2014). "Robert Gates: Most Countries Conduct Economic Espionage". *The Diplomat*, Available on https://thediplomat.com/2014/05/ robert-gates-most-countries-conduct-economic-espionage/ (Accessed August 20, 2021).

15. Kim, I. Kuljis, J. (2010). "Applying Content Analysis to Web based Content", *Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces*. Cavtat. Croatia. p. 283-288.

16. Lederman, N.G. Lederman, J.S. (2015), "What Is A Theoretical Framework? A Practical Answer", *Journal of Science Teacher Education*. Routledge. Chicago. 26(2). p. 593-597.

17. MacDonald, S. Headlam, N. (2008), "Research Methods Handbook", CLES, Manchester.

18. Murman, E. (2007). "Introduction to Lean Six Sigma Methods. Lecture Notes". *MIT Open Courseware*. Available on https://ocw.mit.edu/ courses/aeronautics-and-astronautics/16-660j-introduction- to-lean-six-sigma-methods-january-iap-2012/lecture-notes-1/ (Accessed August 20, 2021).

19. Norman, J. (2011). "WikiLeaks: France Leads Russia, China in Industrial Spying in Europe", *CBS News*. Available on https://www.cbsnews. com/news/wikileaks-france-leads-russia-china-in-industrial-spying-in-europe/ (Accessed August 20, 2021).

20. Olson, D.L. Lauhoff, G. (2019). "Descriptive Data Mining". Springer. New York.

21. Pasquazzi, S. (2017). "Economic Intelligence", *Economic Warfare. Storia de'l Arma Economica*. Società Italiana di Storia Militare. Milano. p. 499-514.

22. Patil, V. (2013). "A Review of DFSS". *International Journal of Innovations in Engineering and Technology*, 2(1), p. 369-375.

23. Pyzdek, T. (2003). "*The Six Sigma Handbook"*. Mc Graw-Hill. New York.

24. Rawnsley, A. (2013). "Espionage? Moi?" *Foreign Policy*. Available on https:// foreignpolicy.com/2013/07/02/espionage-moi/ (Accessed August 20, 2021).

25. Reid, M. (2016). "A Comparative Approach to Economic Espionage". *University of Miami Law Review*, 70(3), p. 757-829.

26. Roper, D.S. (2002), "Are All Semi-presidential Regimes the Same? A Comparison of Premier-Presidential Regimes". *Comparative Politics*. 34(3), p. 253-272.

27. Uslaner, E.M. (2018), "The Oxford Handbook of Social and Political Trust". Oxford University Press. Oxford.

28. Ungureanu, G.T. (2020), "Evolutions, trends and essential characteristics of economic intelligence systems", *Scientific Report*, Library of "Mihai Viteazul" National Intelligence Academy. Bucharest.

29. Ungureanu, G.T. (2021), "Comparative Analysis of the United States of America and France National Economic Intelligence Systems", *Scientific Report*, Library of "Mihai Viteazul" National Intelligence Academy. Bucharest.

30. Walliman, N. (2011), "Research Methods. The Basics". Routledge. Abingdon.

31. Wasserman, S. Faust, K., (1994). "Social Network Analysis: Methods and Applications". Cambridge University Press. Cambridge.

32. Thijs, N. Hammerschmid, G. Palaric, Enora. (2017). "A comparative overview of public administration characteristics and performance in EU280", European Commission. Brussels.

33. *** French Presidency. (2017). "Defence and National Security Strategic Review". *National Security Strategy*, French Presidency, Paris.

34. *** ieee. (2003). "Economic intelligence in a global world". *Strategic Dossier 162 B*. Spanish Ministry of Defence, Spanish Institute for Strategic Studies. Madrid.

35. *** France 24 – News Wires, (2011), "France is top industrial espionage offender", *France 24*. Available on https://www.france24.com/en/20110104-france-industrial-espionage-economy-germany-russia-china-business (Accessed August 20, 2021).

36. *** MacArthur. General Staff. (1994), "Reports of General MacArthur. MacArthur in Japan. The Occupation: Military Phase". Library of Congress. Washington.

37. *** ONCE – Office of the National Counterintelligence Executive. (2011). "Foreign Spies Stealing US Economic Secrets in Cyberspace". E*conomic Intelligence Report*. Washington.

38. *** Tarlogic. (2019). "France and economic intelligence." Available on https://www.tarlogic.com/blog/france-and-economic-intelligence/ (Accessed December 18, 2020).

39. Zandee, D., and Kruijver, K. (2019). "The European Intervention Initiative". *Clingendael Report*. Netherlands Institute of International Relations "Clingendael". Hague.

COOPERATION BETWEEN INTELLIGENCE OFFICIALS AND DECISION-MAKERS: THEORY VERSUS PRACTICE

Mădălina-Elena LUPU*

Abstract:

This article focuses on the cooperation between intelligence officials and decision-makers in the briefing process, by juxtaposing theory with practice. It aims to analyse the process of cooperation from a dual perspective, in order to identify the advantages and disadvantages of briefing, to identify the factors that influence the process and, in the end, to offer suggestions for cooperation improvement. Communication in this area is essential not only for the two actors and the organizations they represent, but for citizens and for national security as well.

The paper begins by distinguishing between information and intelligence, with the relationship between intelligence officials and decision-makers through the briefing process, in order to highlight the necessity and importance of cooperation and to establish at the same time a theoretical basis. It continues with the advantages and disadvantages of briefing and of direct cooperation instead of sending the message without messenger, with the factors that prove to influence cooperation in practice. Last but not least, the article puts forward a series of suggestions for the improvement of cooperation.

Ultimately, intelligence efficiency depends on both the decision and decision-makers. Direct and indirect cooperation is influenced in practice by objective and subjective factors, by the harmonization of the two different groups, by the availability of decision makers, by an intelligence and political culture, by a cooperation based on mutual trust, by paying attention to the intelligence provided, as well as to the messenger, and by reducing the all-knowing perception of decision-makers.

Keywords: *intelligence, decision-makers, cooperation, national security, briefing, intelligence product*.

* PhD student, "Mihai Viteazul" National Intelligence Academy (MVNIA), Romania, email: lupu.madalina@animv.eu

Introduction

To make a distinction between information and intelligence, it is important to understand that information represents "raw data, lacking context or coherence" (Crump, 2015, p. 5), while intelligence is much more than information. Intelligence results from "the process of information analysis or evaluation" (Gill & Phythian, 2018, p. 69), in other words from the evaluation of those primary, unprocessed, incomplete and illogical data that are collected in the first stage by intelligence organizations. In a second stage, the collected data is transformed into intelligence with the help of analysts. Intelligence analysts are those "magicians of knowledge who transform information into intelligence" (Coldea, 2017, p. 52), but not through *magic* methods, in order to provide a "current and previous knowledge of the world around us" (Johnson, 2017) to which we can add for a *future knowledge of the world* that is absolutely necessary for decision-makers and for national security.

After this current, previous or future knowledge is obtained, in a third stage, the intelligence organizations must inform the decision-makers about it. This process is called the briefing process and is defined as being "the specialized activity of elaborating the briefing documents and sending them to legally authorized customers" (Nițu, 2011, p. 72). This is one of the ways intelligence organizations contribute to a state's national security, but in order to do that the two actors involved in this process must cooperate. As a basic role of intelligence, this contribution represents *the sine qua non* condition of an intelligence organization and depends on many factors, including cooperation.

The briefing activity can be considered the central element between the knowledge provided by intelligence organizations and the power exercised by decision-makers. Decision-makers are those customers of intelligence, who are legally authorized in this regard and responsible for the decision-making process in the field of national security. They cannot have or acquire expertise in all the problems they cope with in the exercise of power, so the provided intelligence is intended to facilitate their decision-making process when data is

missing and especially in cases when their data is insufficient, incomplete, invalidated or biased.

The decision act generally implies two elements which depend on each other, "an act of will and the existence of alternatives" (Dente, 2014, p. 5). Particularly, intelligence organizations, through briefing, formulate these alternatives for decision-makers, while they have the responsibility to choose one or none of them in the decision-making process. Thus, the act of will belongs to the decision-makers, while the activity of finding possible alternatives belongs to the intelligence organizations.

Intelligence can have a dual role in the decision-making process, ante and post-decision, so intelligence can be considered, in the beginning, "a basis for decisions" or, in the end, "a witness to the consequences of decisions". The outcome of choices made by decision-makers is influenced by two major factors; on the one hand, by "the ability of intelligence to understand reality" and, on the other hand, by "the ability of decision-makers to understand intelligence analysis" (Maior & Nițu, 2013, p. 24), to which we can add that the cooperation between the two actors is necessary for decision-makers to *grasp the understanding* and for intelligence organizations to explain the understanding. The national security of a state depends on the abilities of these actors.

In theory, this role of intelligence is familiar to both actors, but this is not enough for national security. In practice, the process of collecting and providing intelligence to decision-makers can prove useless if it is not understood and materialized into a decision; therefore, intelligence efficiency is conditioned by decision. In other words, "no matter how brilliant the intelligence performance, the nation will have failed if no action has been taken" (Grabo, 2010, p. 26). It will also be a waste of time and resources for intelligence organizations if decision-makers do not take into consideration intelligence provided or if intelligence proves to be useless for the decision-making process.

Given that intelligence is a key tool in decision-making and that its effectiveness is conditioned by decision-making, communication between both actors involved in the process is mandatory because

"there is simply no way to put intelligence to good use" (Johnson & Wirtz, 2011, p. 191). Because, many of the failures in intelligence were "due to the absence of a common language and a real and efficient communication" (Maior, 2010, p. 54) between them and given that "there is no phase of the intelligence business which is more important than the proper relationship between intelligence itself and the people who use its products" (Johnson & Wirtz, 2011, p. 140), we consider that the issue of cooperation between intelligence officials and decision-makers in the briefing process is not only a challenge and an opportunity for all the parties involved in the process, but also a necessity for national security of any state.

In Romania, this cooperation is not sufficiently analysed due to the fact that intelligence studies are still in their infancy and they are marked by the myth about secret services, compared to the scientific advancements of the field in countries where there is already a tradition of over five decades. In order to address this shortcoming, as well as the need, timeliness and direct applicability of this cooperation to the intelligence and national security of any state, this article aims to analyse the cooperation between intelligence officials and decision-makers in the briefing process using comparative analysis. The approach will be based on a dual perspective, theoretical and practical, and will intend to identify in the beginning the advantages and disadvantages of briefing ways, then the factors that influence the process and eventually to identify suggestions for cooperation improvement.

Ways of briefing: advantages and disadvantages

In the process of maintaining national security of a state, decision-makers rely on intelligence organizations to provide them with the best intelligence. In this regard, intelligence analysis becomes the basic element through which intelligence officials cooperate with decision-makers indirectly through intelligence products or directly through briefing, in order to contribute to national security decisions. Before these ways of briefing are used, questions arise, such as: what is the best way of briefing, direct (visual or auditory) or indirect, detailed or concise? Donald Trump, former president of the United States of

America, opted for the visual instead of the auditory and for the short instead of the details, as follows: "He reportedly prefers images and maps over long, drawn-out analyses. Analysts have been told to keep reports short and simple, no longer than a page per topic." (Gill & Phythian, 2018, p. 184)

Regarding the best way of briefing, directly through the oral briefing or indirectly through the sending of intelligence products, it is noted that "the main reason many policy officials prefer oral briefings to written products is because they welcome the opportunity to «cross-examine» the analyst, probing for what he or she knows that could be helpful in making decisions amidst inevitable uncertainty" (George & Kline, 2006, p. 299), which is an informational and decision-making advantage for decision makers. The oral briefing option is also an advantage for intelligence officials, who thus have the opportunity to clarify some aspects that are not included in the intelligence product or explain those on which the product is based. The first known use of *briefing* took place in 1904, in the meaning of "an act or court that provides exact instructions or essential information" (Dictionary, Merriam-Webster).

Intelligence products are the basis of briefing and they result from the process of analysing and evaluating information, through which they are validated, given a meaning and placed in a context, to be provided to decision-makers and integrated into the decision-making process. The decision-maker is not only a passive receiver of intelligence, but an active one who has the possibility and the responsibility to transform intelligence into decision and action. In the United States of America, the President's Daily Brief (PDB) is "likely the most influential and as former actionable current intelligence publication" produced by the Intelligence Community. Its major importance was expressed by the former director of the Central Intelligence Agency (CIA), Robert Gates, as follows: "writing for the PDB (...) was the reason for our existence" (George, 2020, p. 181-182).

Former US president George H. W. Bush used the oral briefing constantly, stating that: "each working day as president I invited CIA briefers to sit with me, enabling them to offer insights beyond those on the PDB's pages and to answer my questions" and as a result "without

fail, they enriched my time with the PDB and helped me make more informed choices about world affairs" (Priess, 2016, p. 8). Thus, he can be considered a worthy example to be followed in this cooperation process, because he gave a major importance to intelligence organizations and in this way he offered them the possibility to contribute to national security decisions. A useful element is the fact that George H. W. Bush had a double quality, intelligence provider through the position previously held by director of the CIA and decision-maker, being president of the USA. As a result, he understood the interdependence between intelligence and decision, as well as the imperative of cooperation, and was a *binder* that facilitated the *harmonization* between intelligence and decision for the benefit of national security.

Over time, the format of the *President's Daily Brief*, its content and delivery way has gone through various transformations, has been adapted and customized to each president and has gone from printing on high quality paper to loading on a secure tablet, given the advanced technology. Although inherent changes have taken place, it is important to mention that the intelligence presentation in another form does not minimize the need for cooperation between intelligence officials and decision-makers, but remains a constant and indispensible element, regardless of format.

Sending the *message without a messenger*, or Sending only the intelligence product to decision-makers, it can prove to be a disadvantage as "a conversation may be more important than a paper". In this briefing process "«customers» are becoming «clients» to be served in ongoing relationships, not serviced at arm's length with products, raising analogies between lawyers and clients, or doctors and patients" (Agreel & Treverton, 2015, p. 136). If in the relationship between lawyers and clients the stake is freedom and between doctors and patients the stake is health and even life, in cooperation between intelligence and decision-makers the stake is national security.

The message sent without a messenger, metaphorically speaking, also has the disadvantage that there is no certainty of its understanding. The intelligence product risks not being understood not only because of the inability of decision-makers to decrypt it, but also

because of the inability of intelligence organizations to formulate the message clearly and completely. Another disadvantage is the interpretation of decision-makers, which could be different from the intended one and thus could lead to a decision failure.

Influencing factors in cooperation

In theory, cooperation between these two different institutions whose functions converge towards the same goal, to ensure the national security of a state, is mutually agreed and its imperative is obvious, but in practice the cooperation process faces various influencing factors which can have repercussions on the intelligence process, on the one hand and on the decision-making process, on the other hand. Cooperation, in general terms, may be formal or informal, easy or difficult, effective or ineffective depending on objective factors, such as: the level of democracy in the state, the horizontal or vertical organizational system, the geographic location, the available resources; or on subjective factors like: the level of interest in cooperation, the respect for national values and principles and the cultural influences that have repercussions on the way the two actors relate to one another regarding the attitude of superiority, inferiority or equality.

At the same time, cooperation can be influenced by the history of collaboration of the two institutions regarding previous successes and failures, the personality of the actors involved, the level of education, the level of competence acquired, the ability of persuasion and active listening, the level of interest, as well as the gender and age of the cooperating actors. It is important to mention that all these factors, along with the objective and the subjective ones, already exist when the process of cooperation between the new intelligence officials and the new decision-makers begins. When the process of cooperation is initiated, other factors appear and can influence its progression, namely: their origin from *different groups* that promote different cultures, the *urgency* of the policy in contrast to the intelligence process that requires time to materialize, the non-existence of an *intelligence culture* and a *political culture*, the lack of trust, the fact that intelligence can be ignored or that decision-makers can prove to be *omniscient*.

Although both actors have the same national culture, they practically come from two different *groups*, two different organizations that share different cultures and values. However, in terms of responsibilities the officials of these *groups* have, they must cooperate and harmonize these different cultures and values. Robert Gates has noticed in practice, which is valuable, "how different the intelligence and policy cultures are and how valuable it could be for intelligence to get close to consumers" (Treverton, 2004, p. 205). This noticed comparison and recommendation that has been made by Robert Gates is based on his double expertise in both the intelligence and decision-making areas.

In theory, time is equal for all people, but in practice it is perceived differently by the two actors through the lenses they look at and through the urgency of politics in contrast to the long process of intelligence. If decision makers expect practical and immediate results from intelligence, in contrast, intelligence organizations tend to see things from a broader perspective before narrowing it down and not see things only in the short term, but in the medium and long-term as well. Decision-makers have an inherent tendency to focus on pressing issues, while intelligence organizations make connections between the past (the background of the problem), the present (motivation, objectives, risks, opportunities) and the future (identifying variables, consequences, trends and developments). For intelligence organizations time is relevant, because it can confirm or not certain connections between problems and solutions or can validate anticipated developments, while decision-makers cannot delay the decision-making process.

In practice, "the dominant problem for decision-makers in using intelligence, however, remains time" because no matter how interested may they be, "they never have enough time to read as much as they would like" (Betts, 2007, p. 70). An explanation and a justification at the same time is the fact that "the decision-maker's imperative is political: to make decisions and produce results, to act quickly and with confidence" (Betts, 2007, p. 69). Under these conditions, intelligence in order to be useful for decision-makers "must arrive at the right time, which is after the leaders have become seized with the problem but

before they have made up their minds", this interval actually being "a narrow window" (Jervis, 2010, p. 167).

Ideally, when decision-makers offer intelligence officials enough time to provide arguments for intelligence products and to provide further clarification, another problem might appears, i.e. the *absence of an intelligence culture* of decision-makers that affects the understanding of the intelligence provided, the intelligence activity as a whole, the decision-making process and the national security. For the decision-maker to have an *intelligence culture* depends on the involvement of both actors. If an *intelligence culture* does not exist, we can wonder if intelligence organizations can make up for it. Also, it is our contention that *intelligence culture* should be introduced as a mandatory condition for decision-makers in the exercise of national security decision-making powers.

Intelligence organizations should, in turn, have a *political culture* in order to understand the decision-making process and to communicate more easily with decision-makers. In practice, to become relevant for the decision-making process, intelligence must be based on "knowledge (...) of decision-making mechanisms, the political area to which his assessments go the security agenda and the expectations of intelligence customers" (Maior & Nițu, 2013, p. 34). In theory, if enough time is allocated for intelligence, if decision-makers have a *culture of intelligence* and intelligence organizations have a *political culture*, then another factor – *trust* –might appear in the process of cooperation. Trust can be seen as trust of intelligence officials in decision-makers and in their judgement and trust of decision-makers in the capabilities of intelligence organizations, as well as in the impartiality of intelligence products.

Trust is generally known to be "a fundamental key to any social interaction" (Akhgar & Yates, 2013, p. 81). Practically and particularly, the interaction between intelligence officials and decision-makers implies a very high degree of responsibility, compared to the social one, and implicitly a directly proportional degree of trust for the major reason that it involves the national security of a state. Therefore, sometimes, "clear statements about the level of confidence are even more important than the judgments themselves, especially if the

confidence level is low" (Fingar, 2011, p. 36-37) in order to maintain an indispensable basis for cooperation.

Florian Coldea considers trust to be "the key to the institutional relationship between the organization (intelligence) and its customers (decision-makers)", given the fact that "the level of trust is, from a certain perspective, directly proportional to the results of the activity". When there is mutual trust, the result is a win-win relationship: "customers will be more confident if they receive consistent and timely information", while intelligence organizations "will have more trust if they really use them" (Coldea, 2017, p. 108) in the decision-making process. Intelligence officials can prove their trust in decision-makers "by demonstrating knowledge, utility, and discretion" (Fingar, 2011, p. 33).

In practice, "having all of the most objective information in the world will not matter if the president and his inner circle operate without giving serious attention to it, and they will not pay much attention unless they interact frequently and have rapport with the intelligence leadership" (Betts, 2007, p. 138). This intelligence *ignorance* by decision-makers minimizes the contribution of intelligence to the decision-making process and, together with the other factors addressed, can have repercussions on national security. An eloquent example of intelligence *ignorance* is Donald Trump who at the beginning of the presidential term did not pay (enough) attention to the intelligence function. Subsequently, he requested the presence of national security advisers "to be nearby most days" (Gill & Phythian, 2018, p. 184), but this later attitude cannot compensate for the former intelligence ignorance and, at the same time, shows two important facts, the power of decision-makers and the limits of intelligence organizations.

This *ignorance* might be "the greatest paradox of intelligence", because intelligence organizations allocate time and resources and take major risks to create intelligence products related to national security, only "to have them (decision-makers) ignore it" in the final stage (Johnson, 2015, p. 8). Moreover, there are cases when policymakers are "prone not only to reject intelligence but to scorn the messenger" (Jervis, 2010, p. 167). Intelligence could also be ignored due to the fact that "decision-makers are, almost by definition, busy people who will

not spend much time reading classified products (…) to find out what they already know" (Fingar, 2011, p. 85). This *omniscient* attitude shown by the decision-makers can have a negative impact on cooperation with intelligence officials, can limit the efficiency of intelligence in the decision-making process and can be vulnerability for national security.

Suggestions to improve cooperation

Intelligence organizations "cannot reach a level of knowledge that allows them to answer key questions of security policies, if they do not interact in one form or another with the decision-maker" (Maior & Nițu, 2013, p. 34), but this is in theory. In practice, cooperation proves to be "difficult and winding and always must be validated, always supported and defended". No matter how important and difficult this process proves to be, intelligence organizations are "the only ones that can determine a victory or a failure of the state in the field of security" (Maior, 2010, p. 31), thus cooperation shouldn't be *an option*, but *a must* just as national security is.

Cooperation between intelligence officials and decision-makers is influenced by factors that affect the efficiency and contribution of intelligence to decision-making processes and national security. Thus, the *harmonization* of the two different *groups*, the availability of decision-makers, an *intelligence culture* and a *political culture*, building and strengthening cooperation based on mutual trust, paying attention to the intelligence provided and the messenger and reducing the perception of omniscience would facilitate the process of cooperation and would bring benefits for both parties involved, for the national security and the citizens, by ensuring a secure climate that allows them to exercise their rights and freedoms.

George H. W. Bush is an example of this type of cooperation, as he has practically understood how the intelligence and decision-making process works, having an *intelligence culture* and acquiring a *political culture* through his functions. He gave time to intelligence officials through constant discussions with briefers, he started from the premise of trust in this cooperation process, he did not ignore intelligence, but gave it due attention and did not show *omniscience*, but openness to

unknown knowledge. In this way, he practiced a triple-win form of cooperation, for the intelligence process, for the decision-making one and for the national security of the USA.

Having an *intelligence culture* already was one of the exceptions and an advantage for the former president, an advantage which *paved the way* for cooperation. This advantage can be achieved not only as being part of the intelligence activity, but also by showing openness, availability, responsibility and interest in learning what intelligence can do for national security. In cases of non-cooperation, another decision-maker suggested that the following measures should be taken to improve cooperation between intelligence and decision-makers, "to identify the decision-makers who count, to approach them because they are just too busy, to study them from all perspectives, to take the initiative to establish ties by letting them know what can intelligence do for them in its area of expertise, to customize intelligence papers and briefings, to understand the other side by visiting them and to create a win-win relationship" (Johnson & Wirtz, 2011).

Most of these measures involve the initiative of intelligence organizations, identifying and addressing decision-makers, making a complete profile for them, describing what they can do, customizing the products provided and knowing the decision-makers' perspective. *Creating a relationship* involves the participation and involvement of both actors; thus, in this process, the decision makers' involvement is absolutely necessary, their openness, their requests, their own points of view and their active listening, all at the same time.

In this relationship it is difficult to develop a way of cooperation that combines closeness and an independence at the same time, *closeness* that would facilitate cooperation and *independence* that would ensure the objectivity of intelligence. It is essential to establish where independence ends and where the closeness between the two actors begins, what is allowed and what is forbidden and to provide regulations to sanction their violation, as well as recommendations to improve cooperation, because "improving the way this relationship works, represents the key to a nation's success" (Megheşan, 2013, p. 230). A recommendation identified in the literature indicates a *distant approach*, as follows: "the best arrangement is for intelligence and

politics to be in separate but adjoining rooms with communicating doors and thin partitions walls (...)" (Dover, Goodman, & Hillebrand, 2014, p. 70). This metaphorical indication involves a physical *separation* which exists in fact, but also a *proximity* that would allow them to cooperate, but this *separation* and *proximity* are difficult to be quantified and respected in practice.

Conclusions

Intelligence organizations obtain intelligence while decision-makers make decisions. There is an interdependent connection between the two parties involved in the process of ensuring national security, so that the efficiency of intelligence is conditioned by the decision. The national security of a state depends on how intelligence organizations *understand reality* and how decision-makers *grasp how it is understood by* intelligence organizations. This process of *grasping the understanding* involves, in theory and practice, cooperation between intelligence officials and decision-makers, i.e. between those who have obtained the understanding and those who have the opportunity to use it in the decision-making process.

Indirect cooperation, which involves sending only the intelligence product to decision-makers or the *messenger without message*, compared to direct cooperation proves to be absolutely necessary in theory, but not enough in practice, because the intelligence product *does not speak for itself* in all cases and because clarifications and additional information are meant to clear the misunderstandings. In practice, both direct and indirect cooperation are influenced by both objective and subjective factors, by the harmonization of the two different *groups*, by the availability of decision-makers, by an *intelligence* and *political culture*, by building and strengthening cooperation based on mutual trust, by paying attention to the intelligence provided, as well as to the messenger and by reducing the omniscient perception of decision-makers.

It is through cooperation between intelligence officials and decision-makers that intelligence organizations and intelligence itself can contribute to the decision-making process and to national security, because intelligence and decision depend on each other. This

cooperation, in practice, must combine closeness and independence at the same time; the former facilitates cooperation and an independence that ensures the objectivity of intelligence and decision, but finding the perfect balance may sometimes prove to be a challenging task.

References:

1. Agreel, W., Treverton, G. (2015). *National Intelligence and Science. Beyond the Great Divide in Analysis and Policy.* New York: Oxford University Press.

2. Akhgar, B., Yates, S. (2013). *Strategic Intelligence Management. National Security Imperatives and Information and Communications Technologies.* Boston: Elsevier.

3. Betts, R. K. (2007). *Enemies of Intelligence. Knowledge and Power in American National Security.* New York: Columbia University Press.

4. Coldea, F. (2017). *Despre serviciile de intelligence – gânduri, perspective, opinii. Pledoarie pentru încredere.* Bucureşti: ANIMV.

5. Crump, J. (2015). *Corporate Security Intelligence and Strategic Decision Making.* Boca Raton: CRC Press.

6. Dente, B. (2014). *Understanding Policy Decisions.* Milan: Springer.

7. Dover, R., Goodman, M. S., Hillebrand, C. (2014). *Routledge Companion to Intelligence Studies.* New York: Routledge.

8. Fingar, T. (2011). *Reducing Uncertainty. Intelligence Analysis and National Security.* Stanford, CA: Stanford University Press.

9. George, R. Z. (2020). *Intelligence in the National Security Enterprise: An Introduction.* Washington, DC: Georgetown University Press.

10. George, R. Z., Kline, R. (2006). *Intelligence and the National Security Strategist: Enduring Issues and Challenges.* USA: Rowman & Littlefield Publishers, Inc.

11. Gill, P., Phythian, M. (2018). *Intelligence in an Insecure World* (ed. Third Edition). Cambridge, Medford, MA: Polity Press.

12. Grabo, C. (2010). *Handbook of Warning Intelligence: Assessing the Threat to National Security.* United Kingdom: Scarecrow Press, Inc.

13. Jervis, R. (2010). *Why Intelligence Fails. Lessons from the Iranian Revolution and the Iraq War.* Ithaca, London: Cornell University Press.

14. Johnson, L. K. (2015). *Essentials of Strategic Intelligence.* Santa Barbara, CA: Praeger Security International.

15. Johnson, L. K. (2017). *National Security Intelligence. Secret Operations in Defense of the Democracies* (Second edition). Cambridge, UK, Malden, USA: Polity.

16. Johnson, L. K., Wirtz, J. (2011). *Intelligence. The Secret World of Spies. An Anthology.* New York: Oxford University Press.

17. Maior, G. C. (2010). *Un război al minții. Intelligence, servicii de informații și cunoaștere strategică în secolul XXI.* București: Rao.

18. Maior, G. C., Nițu, I. (2013). *Ars Analytica. Provocări și tendințe în analiza de intelligence.* București: Rao.

19. Megheşan, K. (2013). *Politica externă. Cum o analizăm?* București: Academia Naţionala de Informaţii "Mihai Viteazul".

20. *Dictionary Merriam-Webster*. Available on www.merriam-webster. com/dictionary/briefing și https://www.merriam-webster. com/dictionary/ briefing.

21. Nițu, I. (2011). *Ghidul Analistului de Intelligence, Compendiu pentru analiștii debutanți.* București: Academia Națională de Informații "Mihai Viteazul".

22. Treverton, G. F. (2004). *Reshaping National Intelligence for an Age of Information.* United Kingdom: Cambridge University Press.

INTELLIGENCE IN SOCIETY: SPARKS OF A SYSTEMIC APPROACH

Iulian ONEAŞCĂ*

Abstract:
The article addresses the potential role of intelligence structures in social change, aiming to support the economy of effort as a prerequisite for maximizing societal efficiency. Western democracies, with their openness to dialogue, provides the supporting arguments. The theme and its objective, respond to specific concerns of the policy-making forums, serving active social forces. The evolution of society is addressed through economics, considering market mechanisms in the pursuit of exchanges, with socio-human energy expenditures and harvesting. The approach is multi-methodological, based on an economic interpretation of the theory of social systems, supported by heuristics and casuistic. The enterprise is based on the analytical reflection of socio-human behaviour, consisting of capital-forming assets. The intelligence activities are central to the system. Surveillance and information collection activities are oriented towards the concentrations of social capital and power. The progression (information analysis, intelligence cooperation) of the evolution of society (identity change) arises from the responsibility of intelligence towards society and diverse opportunities (the power of knowledge, policy-driven evolution). The results are varied and differentiated: from concepts (counter-reaction), a systems theory adapted to the real world, methodological elements to orient information analysis, and substantiated suggestions useful for the development of public policies, to foreshadowed identity options. Building better at home remains a matter of major concern due to traditions that favour reforms, to the detriment of an adaptation system.

Keywords: *society, systems, human energy, power, intelligence*.

Introduction

The article addresses the potential role of intelligence structures in social change, aiming to support the economy of effort as a

* PhD in economics and expert in EU's social models and processes within the European Institute of Romania, e-mail: iulian.oneasca@gmail.com

prerequisite for maximizing societal efficiency. In particular, the paper aims to: contribute to improving the perceptions and transparency with regard to the role that intelligence can play in supporting the evolution of society; suggest a comprehensive framework for the analysis of information. In addition, the work draws attention to the perils of domestic politics.

The topic of the paper and its objectives, respond to specific concerns of the policy-making forums, serving political and other active social forces. The evolution of society is addressed through economics, considering market mechanisms in the pursuit of exchanges, with socio-human energy expenditures and harvesting. The approach is pluri-methodological, based on an economic interpretation of the social systems theory, supported by heuristics and casuistic. Simplification, necessary to reduce uncertainty, is complemented by *complexification*, to focus the analysis and to allow for the simultaneous treatment of several topics of interest. Western democracies, with their openness to dialogue, provide the supporting arguments.

The analysis calls for the wisdom of universal and specialized literature and capitalizes on history lessons, drawn from developments of hundreds of years and global coverage, or newer ones, with regional relevance.

The paper selects and treats various elements:

i) basic theories and concepts, for the development of a framework, adapted to the real world;

ii) practical support for the reflection of the social system (social energy, principles, and social dimensions), and of its functioning (economy, assets, capital);

iii) objectives and means (societal efficiency, power, politics and democracy);

iv) progression (information analysis, intelligence cooperation) of the evolution of society (identity change), responsibility of intelligence towards society, and diverse opportunities (power of knowledge, policy-driven evolution).

The results acquired vary and differentiate in terms of accuracy and applicability: from well-outlined notions, such as concepts,

patterns, tendencies and rational public policy suggestions, to foreshadowed identity development options.

The paper considers two specific elements, with differentiated roles and priorities, which produce distinct, complementary results, in accordance with the specific objectives. The analysis is organised accordingly, in two main parts.

a) The first one – *A systemic understanding of intelligence in society* – is a methodological work oriented towards creating a framework for analyses, with clear concepts, principles and theories. Amongst the results there are *a systems theory adapted to the real world,* a social system with energies and powers, integrated into a system of systems, and suggestions regarding the understanding of intelligence.

b) The second part – *guiding a systemic approach of intelligence in society* – illustrates the use of previously developed framework. It reveals the potential role and contributions of intelligence in tackling society`s economy of effort. The main results consist of a concept (counter-reaction); practical steps to orient information analysis towards power centres, according to needed skills and the fields of observation – dimensions and subsystems; reasons for the intelligence forces to join efforts; reasonable arguments for the involvement of intelligence agencies in changing the identity of society and their potential role.

A modified version of the theory of social systems (Oneașcă, 2018) eliminates the previous shortcomings; it considers the energy and associated principles, respectively the minimum action, self-organization and economy of effort, as elements of continuity of an all-encompassing system. The main functional social dimensions – politics, economy, and justice – house the greatest systemic opportunities and threats, nationally and internationally. Intelligence agencies have a say in this. Society entrusts them with most of its information. In turn, intelligence agencies are obliged to harness their powers and serve society, supporting its policy-driven evolution.

In conclusion, the analyses and the recommendations support and reinforce the self-organization of society. The article suggests solutions to improve the analysis of information and ways to support

systemic modelling of socio-human behaviour and increase the efficiency of society. The intelligence activities are essential.

A systemic understanding of intelligence in society

The adoption of constitutions throughout the 19th century (CCP, 2014), laid the foundations for the accountability of rulers. The protection of sovereigns and those in the leadership of the states has gradually diminished, though it has never been abandoned for good. Privileges have been cloaked in obscure forms (e.g., immunity, exemptions, special treatment), as politicians are the first to benefit from their law-making powers. Nonetheless, the advance of government has accelerated. Institutions have developed, specialized, and strengthened. The process continues nowadays, stimulated, amongst others, by the progress of technology, facilitating an exponential growth of data production.

Processed data (information) provide the means to effectively support the exercise of authority and contribute to the rapid change of the world. Significant changes in methods and means of collecting information created "a demand for new approaches to analysis and intelligence" (UNODC, 2011). On such a basis, the international cooperation of intelligence agencies has increased (FIORC, 2017; Legrand, 2020).

The activity has taken on worrying proportions for some. Information about the collection of data, their nature and mass, slipped to the press (Bauman, 2014). Political personalities, justice systems, and civil societies, have reacted and expressed legitimate concerns regarding the preservation of freedoms and liberties (Allard, 2014; Bauman, 2014). On the positive side, intensified international competition rewards states that achieve their goals (e.g., World Bank, 2021). Their ranking process seems to work in favour of better-informed and organized states (UNDP and MBRF, 2020). Accordingly, intelligence has to adjust. The place of intelligence in society, of their agencies and enlarged networks, needs reassessing. The societal understanding of intelligence activities is prefigured by clarifications, firstly about a systems theory adapted to the real world, secondly, about social systems, their energies and powers, and thirdly, about

ways of perceiving intelligence in society. The first two bring to light elements of a coherent methodology and its practical framework, whereas the third introduces the understanding of intelligence activities and their specificity.

A systems' theory adapted to the real world. Systems theory is a theoretical assessment, widespread in the literature, which provides frameworks for comprehensive examinations of various fields; these include society, its components, interactions, and processes. Different models and variants of the systems theory co-exist. Their perspective is multifaceted, rooted in sciences and disciplines (e.g., natural, social), their subdivisions (management, engineering, and design) or, in specific uses and functions (service systems; viable systems; smart systems; reticular systems). Accordingly, there is an abundant stream of research targeting systems theory, and focusing on their origins, definitions and basic concepts, or complex approaches (Laslo and Krippner, 1998; Mele et al., 2010; Stichweh**,** 2011; Carayannis et al., 2016).

The main advances of the theory date back to the middle of the twentieth century. Firstly, the distinction between system and environment replaced the distinction between whole and part (Bertalanffy, 1956). Differentiation facilitates the approach of the system in its state of integration in the real world, and not as an isolated construction. Secondly, a general theory of self-referential systems, which use own outputs as inputs, redefined the distinction between system, and its environment (Foerster, 1960). It is a major step explaining perpetuity of matter, perennity of life, and their interconnectivity. As result, a meaningful definition of a system refers to a functional group of elements. Functionality assumes a purpose to which the interactions between elements contribute. Therefore, any systemic perspective has a 'system', with parts or structures, as the unit of analysis (Parsons, 1965). The structure of a system is multi-level, organised hierarchically. The supra-systems are ordered according to their influence on the system, whereas the subsystems are just parts that contribute to the system`s finality (Barile, 2006, 2008).

The theory should work if applied to a comprehensive and consistent chain of systems. Such a system of systems is the universe, as it provides a natural anchoring point for the approach: any other system may have a supra-system. Thus, the universe forms an all-encompassing system. It comprises everything and everyone. Specific to the universe is its continuous, uninterrupted motion. Motion equals energy. Therefore, energy is the fulcrum of the universe. It accompanies and conditions all processes and provides the required consistency to the systems. Energy cannot be created or destroyed; the law of conservation of energy states it. However, energy can be harvested, expended, or converted into a different form, until it becomes unavailable (Georgescu-Roegen, 1975). The energy, deeply rooted in matter, constitutes the element of continuity for the entire chain of subsystems. Figure 1 portrays the main systems and their corresponding traits and principles.

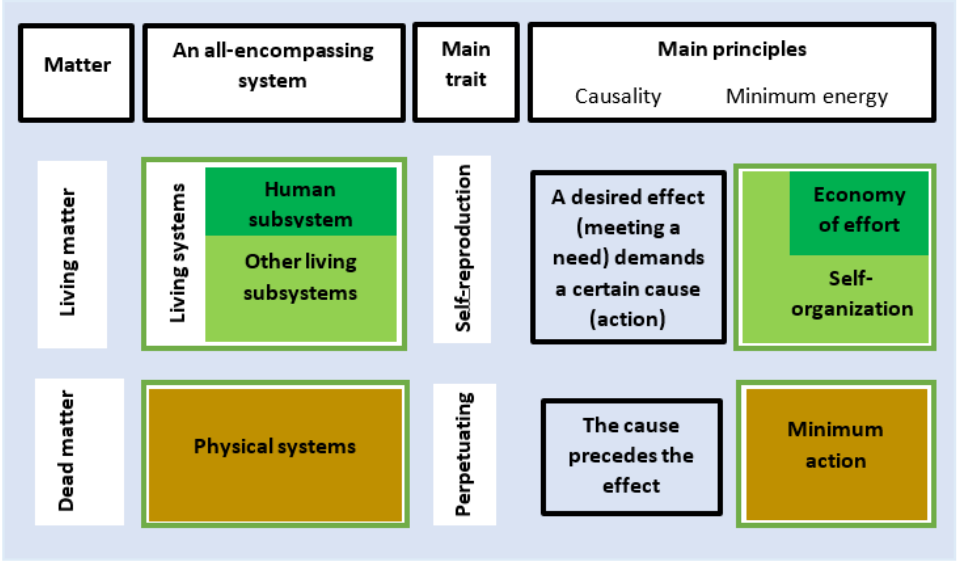


Figure 1: An all-encompassing system *(Source*: the author)

The emergence of living matter comes with the manifestation of a new form of energy, which is subject to specific laws. Living matter

structures living systems. Components of living systems bring free will and its arbitrariness into the material world. The genetic programming of living matter compels communities of individuals and their societies to reproduce. Those who fail to meet such a fundamental requirement, perish.

The principle of minimum action (Maupertuis), governing physical systems, acquires the expression of self-organization (Thelen and Smith, 2006, p. 259; Mathiesen et al., 2011) in living systems. It is the foundation of a new source of legitimacy that involves multiple, reciprocal interactions, exercised at all levels. Instructions of internal (genetic programming) or environmental origin, manage the interactions of individuals and communities (Thelen & Smith, 2006, p. 259).

The evolution of living matter culminates with the emergence of humans. They are endowed with behavioural rationality and possess a certain control over instincts. Thus, people can guide their evolution. A higher form of brain energy feeds their actions and fuels the change. It is what differentiates humans and their societies from other living systems.

Social systems, their energies and powers. The best-known systems theory of society is the social systems one (Luhmann, 1995). It sits on three pillars: systems theory, social evolution theory, and social differentiation theory (Albert, 2016). The social system, as conceived by Luhmann, reduces the complexity and provides a framework for analysis. The social system is a functional construction of components with prescribed limits and environments, characterized by several elements (Luhmann, 1995, p. 15, 17): the system excludes itself from the environment; the environment has no self-reflection or ability to act; the environment is delimited by an open horizon, not by borders that can be crossed.

A two-person subsystem is the simplest social system, as one person cannot meet the condition of being social. Such a social subsystem is included in another subsystem, to ensure broad reproduction. The higher the aggregation, the greater the stability, which no longer depends on the composition or reproduction of a particular subsystem.

The main criticism of the theory of social systems is the lack of a principle or a natural anchor point (Knodt, 1995). This is overcome by considering the universe, as an all-encompassing system, and energy with its principles, as elements of continuity.

Society bases its existence on social relations. These give rise to rules. Social organization structures the existence of communities into activities or areas of existential concern. They form social dimensions, functional (economy, politics, justice), or just existential (less structured, i.e. outlined by human needs). Social dimensions are subsystems in a social system. The more developed they get, the more isolated they become from each other, as a guarantee of their reproduction.

Social systems rely on their capacity for self-reproduction. The perenniality of life involves the harvesting and spending of human energy. Human energy supports i) physical mobility and autonomy; ii) thinking, reasoning, and solving problems; iii) enthusiasm, determination and endurance; iv) the primitive impulse to procreate. It mainly comes from food and is transferred and transformed into various forms necessary for the functioning of individuals and society (WHO, FAO, and UNU, 2004).

Interactions in communities, within and between groups, lead to socialization of energy: individual, human energy becomes social or group energy. Within an all-encompassing system, the energy transferred or converted in the unit of time is power. In social systems, the power expresses the ability of groups and individuals to make others to act in their interest (World Bank, 2017, p. 3).

Human power stems from the innate or acquired capability to mobilize socio-human energy. Communities generate a different kind of power, of social nature. Social power is concentrated hierarchically, multi-level, following the system's structures and activities. Each hierarchy describes a specific power. Among these, the powers generated by the functional dimensions (e.g., political, economic, legal) are the most developed; they cover the entire society. Therefore, power provides a criterion for ranking the quality of energy; it can amplify the effects of its spending, harvesting, or investing.

Each dimension of society has its own markets (e.g., political, economic, and legal). They facilitate the birth and exchange of specific assets and capital (economic, political, and cultural). Culturally, the recurrent exercise of harvesting and spending energy improves traits and substantiates capabilities. Economically, the efforts materialize in goods and services. All these, capabilities, traits, and goods and services represent assets (IAS), which create capital. Assets and capital and can be private, collective, or national and supranational, according to possession. Their expression may use monetary units, or not, depending on whether they emerge on economic or non-economic markets.

Social capital is an aggregation of resources related to a sustainable network of relationships, knowledge, and mutual recognition (Oneaşcă, 2018). Belonging to a group provides each of its members with the support of community-owned (social) capital. The "prerogative" entitles them to credit, in the various senses of the word (Bourdieu, 1986). The existence of hierarchies in the group allows some to benefit more than others, i.e. to approach their share of social capital in various measures.

Much like the social dimensions, the forms of capital are interconnected. For example, cultural capital (scientific or technical) conditions the use of economic capital (e.g. tools).

Capital is energy, embodied or objectified (in the language of Bourdieu, 1986); accordingly, the holders of capital have power. They use it to meet individual or collective needs and desires. The choices that consumers make when purchasing goods and services, as well as when making decisions related to education, work, or politics, all express exercises of power. These become greater with the capital that generated them. Political power, which arises from the collective capital of society as a whole, is the greatest of all. It socializes based on interpersonal relationships and, through them, amplifies, exceeding the sum of the powers of individuals.

Intelligence and its understanding. Intelligence has various meanings and understandings, according to the framework considered: i) real world, portraying the way it is performed (intelligence

providers); ii) legal, based on applicable rules (constitutional foundation and related legislation); iii) academia and society in general, consider perceptions, ideals or desires.

Intelligence activity, like any purposive activity, has a clear criterion of truth, with a technical part, which says whether it works or not, and an economic one, regarding costs, affordable or not. The real worldview of it is implicit and informal, as it relates to applicable expertise. Its understanding, scientific support, or even legitimacy, barely matters; securing the results, or having the job done, is of overriding importance.

The Intelligence Community presents its mission in a formal way, based on understanding the rules. The main activities are "to collect, analyse, and deliver foreign intelligence and counterintelligence information to America's leaders". Based on these "they can make sound decisions to protect" the country. Manuals for analysts (UNODC, 2011) present the intelligence cycle, at both operational and strategic levels (tasking, collection, evaluation of source and data, collation, analysis, inference development, and dissemination).

The legal understanding of intelligence varies depending on the applicable rules. These are specific to diverse institutions and dominant cultures. The wide world has many examples; the more transparent ones are those in advanced democracies. In the US, intelligence is organised as a community. It has collective structures, such as the National Security Council, and Homeland Security Council, coordination ones (Office of the DNI) and a diversity of specialised components (see US PUBLIC LAW 108–458, 2004; CRS, 2020), covering the development and conduct of foreign, defence, and economic policies, and the protection of United States national interests. Operations safeguard many activity sectors, amongst which military, economic, medical, and geospatial ones. They all consider a main group of activities, amongst which, i) surveillance and collection of data, ii) analysis, and iii) dissemination.

In general, like many formal rules governing public life, a legal understanding is inertial and lags behind events, either due to technological advances or due to rapidly evolving needs, capabilities, and expectations in society (see UNCTAD, 2020). Decision-making and

regulation take time. In this respect, it is worth mentioning that the initiation of the reform of American intelligence services took a decade, formidable events and several commissions (e.g., CRCUSIC, 1996; US PUBLIC LAW 108–458, 2004).

Society's understanding of intelligence is, by far, the least clear. A supportive environment requires high social development, strong civic attitudes and adaptable institutions. It is in such refined conditions that problems of control and accountability arise. Although the secret that accompanies intelligence activities casts them under a veil, trust in institutions continues to influence perceptions. As result, understanding of intelligence relates to its impact with the world (Kerke and Hijzen, 2021), the way it communicates to the public (Petersen, 2019), and its changing practices (Petersen and Rønn, 2019). Amongst the core-functions of intelligence, there are (Breakspear, 2013): i) foresight and insight, intended ii) to identify impending change (opportunity and threat).

Guiding a systemic approach of intelligence in society

The evolution of the living world exposes its constitutive diversity. This implies the existence of many life forms and the differentiation of their individuals, ensuring the perenniality of life and species. Differentiation is natural and translates into a wide-range of inequalities.

In society, inequality arises from the variation of natural endowment (biological: physical and intellectual; social: status, class; cultural: traditions) and develops by discriminating access to resources (e.g., funding, education and training, employment), while equality is a perpetual social desideratum (Oneaşcă, 2018). Combating inequality has limited success in any society. This is due to insufficient resources and flawed public policies in addressing work, education and health, housing, and social integration. Worldwide policies are even poorer in this respect. As a result, inequality of individuals is passed on to communities and societies, escalating their division and that of the whole world.

Historically, equality has been restored downwards. Wars, plagues, natural disasters and economic crises have played a major role

(Piketty, 2014), as has population growth (Malthus, 1798). In our days, peace and control of plagues give way to growing inequality. It generates threats and opportunities in terms of security, defence, and the fight against crime, making intelligence activities indispensable.

Reproduction of inequality, both within and between societies, is a major concern. Over the next decade, inequality is expected to explode (NIC, 2012), threatening the social contract in many countries (UN, DESA 2020). In this context, it is no coincidence that the livelihoods of families are redefining the measure of expanding prosperity and economic opportunities as a priority for national security (White House, 2021). More than that, inequality fuels crime and corruption, which generate human and material losses and reduce, in turn, the chances of progress and the disruption of alienation cycles. Thus, the productive potential diminishes. Social energy is not fully valorised, and society's progress is confined. Growing competition and rivalry in the international arena reward efficient societies. Accordingly, the distribution of power across the world is changing**.** Intelligence has a role to play. The systemic approach to intelligence is driven by suggestions on information analysis, the economy of effort, intelligence and identity of society.

Information analysis. Information is essential in reflecting reality. It results from energy exchanges, has value for knowledge, and is, therefore, a capital-forming asset. The information holder has power. The more information there is, the greater the power. Intelligence agencies control access to many sources of information worldwide; useful information makes them very powerful.

Advanced societies are knowledge-based. Their economic, social, and political performances rely on the development of data, information, and knowledge. International institutions, think tanks, and academia constantly emphasize the importance of knowledge and innovation (see UNDP and MBRF, 2020; World Bank, 2021).

In line with the above, a sound analysis of a system requires several elements (Foerster, 1979, p. 8; Easton, 1965a, p. 23-25; 1965b, p. 15–16).

1) A "system" to be observed (e.g., economic, political, legal);

2) An observing or a reference system, which constitutes the "*environment*", the one in which the system is embedded;

3) A "response" or variations in the composition and functioning of the observed system, occurring as effect exerted by external and internal factors of change; and

4) "Feedback", as information-based corrections, initiated by the system`s decision-making.

Thus conceived the analysis, the observer implicitly assumes a low path of ambition and a passive goal; it preserves the system, regardless of the achievement of its functionality. Therefore, another important element that may respond to the need for a system change, is required; it is termed (5) "*counter-reaction"* (Oneaşcă, 2018), and understood as an impulse of energy, which initiates qualitative leaps and drive compulsory increases. The counter-reactions result from decisions that involve a transformation of existing "contracts" between individuals and their social constructions. They differ from normal responses, which are in line with the system and its routines. A profound change of the system may occur abruptly, in the absence of a gradual evolution of the system (quantitative accumulation). The necessary accumulations follow nevertheless, at a pace appropriate to the more or less favourable circumstances.

A systemic approach of societies allows for comprehensive and systematic analyses, needed to increase the prospects of progress. Such an approach should consider various perspectives.

- One is facing researchers and their skills, embracing international standards, such as, i) research and development ones (e.g., FORD in OECD, 2015), ii) education disciplines (e.g., ISCED-F, in UNESCO-UIS, 2014); these standards make up the social sciences and respectively, the social disciplines, which *theorize and approximate knowledge about society*.
- A more complex one is oriented towards the fields of observation and the ways they are defined: iii) social dimensions, structured or functional and less structured; iv) societies' administration and the exercise of power and related activities (e.g., global, regional, central and local

institutional structures); v) national accounts, or vi) any specific assembling.

- Finally, any combination of the above can be used.

Methodologically, the analysis of observation fields can have different angles.

- A longitudinal one groups constructed dimensions:
  - functional ones, e.g., economics, politics, justice (Luhmann, 1995);
  - governance of society, e.g., sectors, industries and groups of activities (see the organization of governance or statistics of OECD, EU, UN, at national or sub-state level);
  - the specifics of change measures, e.g., public policies, on different levels of responsibility, such as economic, employment, education and training, health, environment, public order, crime, defence, justice.
- A transversal one aims at the existential (basic human needs) or constitutive (culture) approach of society:
  - human needs systems,
  - public policy systems, and
  - the culture.
- A particular angle can be defined according to certain needs, aiming at interactions delimited in space and time (ad-hoc constituted).

Processing massive amounts of data, available from electronic communications (e.g., satellite, internet, underwater cables, and terrestrial networks), activities databases (public and private), and archives becomes a challenge. In the background is running a "revolution in technology that poses both peril and promise" (White House, 2021). Emerging technologies, such as artificial intelligence (AI) and quantum computing, "could shape everything" in our lifetimes.

Cooperation of the intelligence structures, whether national, regional or international, paves the way for securing the means in assembling, evaluating and analysing ever-increasing data flows. Therefore, the intensified cooperation of the Western intelligence and of non-state actors seems to follow the path of natural evolution

(self-organisation). Historical trends provide arguments that support the assertion: i) the collapse of hierarchical systems, such as the empires, ii) globalisation, as an increasing integration and interdependence of societies.

The economy of effort. Social energy, accumulated at the level of the system, produces the strongest capital and associated power. Consequently, its uses (social embodiments) originate the greatest possible loss or economy of effort.

The collection and analysis of information spawned by the main sources of power in society are of utmost importance. Therefore, resource allocation priorities need to be developed, and appropriate procedures prepared for possible outcomes. A systemic perspective of the power sources, based on the Ford classification of social sciences is foreshadowed in Figure 2.

The focus on power sources benefits from systems, theories and elements of codification. The representation serves to guide analysis to the power centres, capitalizing on the previous methodology. Of great interest are the amount of capital accumulation and its growth rate.

Social science	**Power system / theory**	**Element of codification (operator)**
Sociology	**Social systems** (Luhmann, 1995)	**Communication**
Economics	**Social models** (Oneașcă, 2018)	**Market / exchange**
Psychology	***Psychic systems***	***Thought / consciousness***
Politics	***Political systems***	***Will / decision***
Law	***Legal systems***	***Rule***

Figure 2: A Socio-human energy approach of power centres
(*Source*: the author, based on analyses and data on social systems)

Society works based on communications. Their surveillance comes naturally: all threats, conspiracies and criminal acts require communications, as do opportunities to strengthen security. Therefore, communications have the potential to expose the social capital that grows hostile to the social order, as well as the intentions of influencers.

Public and private data flows of activity records and their archives complement the communications and facilitate the understanding of reality and the forecasting of its evolution. The power centres approach illustrates a comprehensive perspective on subsystems, theories, and ways of systematic analysis of society so that no opportunity or threat can be overlooked. It takes advantage of the overlap of theory with the reality of functional dimensions. The main pillars of the constitutional checks and balances in society are also covered: legislature through politics, judiciary through law, whereas the executive is governance – at the intersection of social sciences – defined as the process by which state and non-state actors interact to design and implement policies in a context of rules (WB, 2017, p. 3).

The economy provides the necessary resource flows for all other dimensions to self-reproduce. It postulates free access to everyone and conditions material existence. Therefore, it is the biggest concern for all livelihoods. The monetisation of society works in favour of the economy. What does not cost has no value. On such a basis, businesses are conducted. In reality, money is just an approximation of the socio-human effort. A very large part of it is unaccounted for; for instance, unpaid household service work was more than 63% of GDP in UK in 2016 (ONS, 2018).

Besides the longitudinal economic power system, a transversal phenomenon that requires a special attention is the entrepreneurship. It is a major component of any spectacular leaps in economic development (Kirzner, 2009); it expresses a capacity for initiative, exercised by individuals, groups, social constructions, or authorities. Market presence of the entrepreneur has been recognised in all social dimension, not only in the economy but also in politics, culture, education, health, etc. (S)he takes advantage of market opportunities and the distribution of assets, for personal benefit, increasing her/his assets.

Politics is the primary dimension in social systems (Luhmann, 1995). The evolution of society demonstrates its essential role and its ability to transform any other dimension. The main functions of politics are (see Buchanan, 1987; Luhmann, 2000): i) production of binding collective decisions; ii) creating the rules of the game; iii) power generation and allocation.

Traditionally, domestic politics is not a target for intelligence. However, the strategic priorities and actions of politicians have raised democratic concerns (NIC, 2021; Leyen, 2019; Petersen, 2019). In addition, actions by Western leaders have provided sufficient reasons to consider law enforcement in politics (see BCJ, 2017; USDJ, 2019). No one should be considered above the law.

Democracy allows competition and diversity of opinions. The rule of society by the many, in democracy, prevents the abuses of the few. However, power sharing divides the social energy and fragments the long-term evolution of society. Thus, democracy promotes a compromise between the freedom that people cannot do without and the costs of dividing society and of its sinuous course. Essentially, democracy continues to exploit the lack of a system to protect people against their own choices (Oneașcă, 2018). Intelligence can contribute to changing it.

In a democracy, more than in authoritarian regimes, sovereignty belongs to the people. Decision-makers work for the benefit of the people. Only in this capacity, do they have access to intelligence reports and possibly act accordingly. However, poor or imperfect rules and institutions, allow authoritarian regimes to intervene in democratic societies; social networks and exchanges provide the ways (EP, 2021; NIC, 2021). "(T)he four cornerstones of Western democracy – state restraint, pluralism, free media and economic openness – provide openings for hostile external actors to interfere in democratic society through a host of covert, non-military means calibrated to undermine their internal cohesion and accelerate political polarization" (Wigell, 2021). Hostile external actors intervene in elections and choose their future opponents; for them it is more direct and efficient – saving time and effort – than to face the results of free elections afterwards.

The main rules and institutions securing social order in society are occasionally tested and their weaknesses are revealed. The Covid-19 pandemic has come as an unexpected burst of needs and urgencies. The outbreak has exposed not only deficiencies of the health care systems (their readiness and capacity to face pandemics), but also the inertia of major political institutions in developed countries. The reaction of Israeli decision-makers seems an exception; it has emerged quickly, under siege. The authorities have assigned the intelligence agencies the mission of securing medical supplies and instruments, in short supply on the international market. The Israeli intelligence providers have acted swiftly, as a rapid intervention team, responding to the task (Kahana, 2021; Eiran, 2020). The case suggests lessons for other countries. Rapid reactions and the availability of a team for intervention are included.

Most countries have little or no reason to consider national security as part of their identity. However, the need for an operational capacity ready to intervene in the event of a national emergency hampered by global competition conditions must be taken into account. The development of such capabilities is of a *counter-reaction* nature as it acts in the direction of improving the system. It also saves time and effort.

The intelligence and identity of society. Social order lies in both inherited and acquired capabilities. The former is rooted in human biological programming, environment, and social traditions (beliefs, values). The latter is generated by structured interactions and rules, formal and informal ones. Humans and their societies have developed a capacity to drive their evolution, purposely. They do that with growing determination and ever-increasing efficiency. Their self-centred and conflicting goals are fast approaching, weakening innate programming and self-organisation. Consequently, social subsystems can succeed or fail in their reproduction. To date, the most developed societies face a high risk of under-reproduction (UN, DESA, 2019). Isn't that an identity trait worth changing? There are much more, some hidden.

Intelligence production needs to consider the persistence of a way of life, based on old, deep-seated principles and attitudes.

Accordingly, common visions of identity (Anglo-Saxon) and interests of developed countries have established the Five Eyes alliance (FIORC, 2017). Success, based on collective capacity and almost forty diverse public policy networks, has shifted trans-governmental goals from inward looking to global governance (Legrand, 2019; 2020). However, institutions and identities are not easily transferable. They "privilege the `constitutive` characteristics of knowledge, identities and norms that define" their own identity (Wendt, 1992). Recognition of the need for change must be accompanied by consideration of new avenues of progress, as well as ways of implementing them in society. Intelligence activities should focus on the main avenues.

Firstly, the problems of control and accountability generated by increased public–private interactions are likely to lead Western intelligence beyond rule-regulation behaviour. In such cases, capacities for critical judgment become relevant (Petersen and Tjalve, 2018). Manifestations of politicisation of intelligence, in the US (Gentry, 2020) and Australia (McPhee, 2020), show that the clarity of intensions makes the difference. The control, accountability and law enforcement should counteract the disregard of applicable norms, orienting the actions in pursuit of the legitimate interest of the people.

Secondly, the principle of Le Chatelier warns that a system tends to counteract external control attempts (Helbing, 2010, p. 9). Therefore, supporting and strengthening self-organization and self-control through mechanism design (Helbing, D., 2010, p. 10), is the right way to shape the social system through human will; it is also in line with the economy of effort principle. Consequently, institutions should be conceived in such a way as to act following the objectives, expectations and actions of society, which define its ideology. Producers and consumers of information need to share this task.

Thirdly, technology has a dynamising role. "The uptake of architectural principles of *security-by-design* and privacy-by-design in digital technologies" (EC, 2021), paves the way to address the digital future of society. Intelligence must be at the forefront of technological progress, both for strategic purposes (e.g., security and defence) and tactical ones (e.g., data protection, collection and analysis). Advanced countries have regulated this (e.g., White House, 2019).

Information and technology are at the forefront of the new gold standard of society's currency; it is immaterial and without nationality. Market-led forces have created crypto currencies. They hide wealth and its sources. The combination of information, technology, and mechanism design places the evolution of society on solid foundations and all-encompassing considerations; they include what previously could not be suspected to exist. It is the ultimate platform for building a knowledge society. The absence of market forces hampers the promotion of such a strong combination. Society must endure the consequences of its social development until it can ensure that its citizens behave in accordance with self-imposed rules. Changing the rules of the game is the way to go. How could intelligence activities support society`s change?

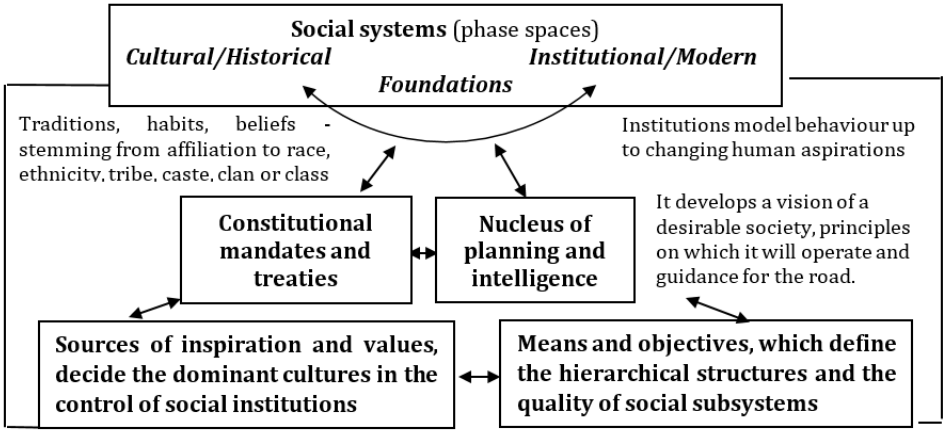


Figure 3: Place of intelligence in identity modelling – Multiple stable attractors
(Source: the author, based on analyses and data on social systems)

Society follows a certain trajectory in its evolution. The predominance of some or other of the influencing factors decides the path. The range of mutations of a social system consists of sets of characteristics or properties towards which the dynamic system tends to evolve. These are called attractors. Groups of attractors define

possible stable states of the system. These, in turn, form multiple system identities or multiple stable attractors (Martin-Breen and Anderies, 2011, p. 15). The identities of the system are part of the set of representations of possible states, called phase spaces. Figure 3 suggests the place of intelligence in identity modelling. Constitutional mandates and treaties provide sources of inspiration and values, pending the definitions of their structures and quality.

Identity modelling involves multidisciplinary and inter-institutional teams that include intelligence expertise. The combined efforts leverage the flows of information (communications, actions, rules, and thoughts) and archives to identify specifics, trends, patterns, and systemic flaws that slow down evolution. In implementing the agencies' initiatives and responsibilities, their intelligence objectives come first (e.g., security and counter-terrorism measures). The more complex enterprises are likely to need preparatory frameworks for cooperation actions inside and across borders. Thus, the need for change and its path are better informed and the decisions prepared.

Discussion and conclusions

The theme is extremely wide to allow for one strong conclusion. There are however several things to mention. Social change in accordance with the principle of the economy of effort sets a high path of ambition. In addition, suggestions for a novel methodology and its use support change. The framework conceived for the analyses of information is robust. The system of systems is universal and can include any real or projected subsystem. Consideration of international standards (social sciences and disciplines, assets) strengthens the way to a comprehensive approach of society. It includes all available data (flows and archives), information and knowledge regarding communications (sociology), actions (economics), decisions (politics), rules (law) and thoughts (psychology). The economic filter to analyse and reflect society is a powerful tool to use. It is not new. However, a unidisciplinary perspective has never been tried. The energy acts as a continuity element of a constitutive nature. It creates conditions to address efficiency in terms of socio-human effort. Therefore, all efforts can be accounted for, monetized or not.

The information available is substantial and ever growing. Orientation of the surveillance and information collection activities towards the concentrations of social capital and power, inside and across borders, saves time and efforts. Better information supports better analysis. Information processing, analysis and capitalization are expensive. Therefore, the cooperation of the intelligence forces in democracies seems imperative. The economy of effort would be significant worldwide. The conditions are favourable; regional and national intelligence strategies share common objectives (e.g., rule of law, democracy, livelihoods, technology) and concerns (authoritarianism, cybercrime, counter-terrorism).

Most of the systemic opportunities and threats faced by intelligence activities are found in the functional dimensions (politics, economics and justice), at national and international level. The larger the social capital, the more reserves it has to improve the efficiency of society. Politics forms the largest of social capitals. It determines the proper functioning of the social system. Politically established rules (decisions and policies) shape society. They reflect energy expenditures of an investment nature; their recursive results accumulate without the need for new expenses. This is a strong reason for intelligence activities to inform them and corroborate them as best they can. In essence, policies must be designed, adopted and implemented for the benefit of the people, not the decision-makers. When in doubt, communication helps.

To date, intelligence activities have a long-established place. In democracy, they serve the national interest and various consumers, support security and defence, avert crime and threat, or, more generally, provide assistance in addressing vulnerabilities and strengthening the social order and its prospects, according to opportunities. However, democracy does not make things easier for intelligence activities; on the contrary, the persistence of varied interests (economic, political) invites authoritarian regimes to exploit the division of society (power and opposition).

Intelligence agencies are very strong players. Societies trust them to access most of the information available. Consequently, they are obliged to harness their powers and serve society, supporting its policy-driven evolution. Still, a strong impetus is necessary. It would

save time and effort if NATO or global governance structures generated it and not urgent needs such as cybercrime, terrorism and pandemic. These are driving countries closer together. Improved rules of cooperation are necessary, accommodating the various cultures. The politics remains indebted.

Deficiencies or even inadequacies of political systems are treated the same, globally: as a constituent part of society, not as a constructed one. Traditions frozen in time favour a long series of reforms, to the detriment of an adaptation system. This remains a matter of major concern. Building better at home is at risk.

References:

1. Albert, M. (2016). *Luhmann and Systems Theory, Oxford Research Encyclopaedia of Politics,* DOI: 10.1093/acrefore/9780190228637.013.7

2. Allard, Tom. (2014). "Australia ordered to cease spying on East Timor by International Court of Justice". *The Sydney Morning Herald*. Archived, on line at https://www.smh.com.au/politics/federal/australia-ordered-to-cease-spying-on-east-timor-by-international-court-of-justice-20140304-hvfya.html

3. Barile, Sergio. (eds.) (2006). *L'impresa come sistema. Contributi sull'Approccio Sistemico Vitale* (ASV), I ed. Torino: Giappichelli.

4. Barile, Sergio. (eds.) (2008). *L'impresa come sistema – Contributi sull'Approccio Sistemico Vitale* (ASV), II ed. Torino: Giappichelli.

5. Bauman, Zygmunt, Bigo, Didier, Esteves, Paulo, Guild, Elspeth, Jabri, Vivienne, Lyon, David, Walker, R. B. J. (2014). *After Snowden: Rethinking the Impact of Surveillance. International Political Sociology* (2014) 8, 121–144, doi: 10.1111/ips.12048

6. Bertalanffy von, Ludwig. (1956). "General System Theory," in General Systems: Yearbook of the Society for the Advancement of General Systems Theory, The Society, online at https://books.google.ro/books?id=rw0DAAAAIAAJ

7. Breakspear, Alan. (2013). "A New Definition of Intelligence", in *Intelligence and National Security*, vol. 28/5, p. 678-693, Routledge, DOI: 10.1080/02684527.2012.699285.

8. Brennan Centre for Justice (BCJ). (2017). *Trump-Russia Investigations: A Guide,* New York University School of Law, online at

https://www.brennancenter.org/sites/default/files/2019-08/Report_Trump-Russia%20Investigations_0.pdf

9. Buchanan, J. M. (1987). "The Constitution of Economic Policy", in American Economic Review. 77 (1987, June): 243-250.

10. Carayannis, Elias G., Campbell, David F. J., Rehman, Scheherazade S. (2016). "Mode 3 knowledge production: Systems and systems theory, clusters and networks", Journal of Innovation and Entrepreneurship, ISSN 2192-5372, Springer, Heidelberg, Vol. 5, Iss. 17, p. 1-24, http://dx.doi.org/10.1186/s13731-016-0045-9

11. Commission on the Roles and Capabilities of the United States Intelligence Community (CRCUSIC). (1996). *Preparing for the 21st Century. An Appraisal of US Intelligence*, online at https://fas.org/irp/offdocs/report.html

12. Comparative Constitutions Project (CCP). (2014). *Relationship between characteristics data and chronology*, online at https://constitution-unit.com/2014/04/23/new-data-available-from-the-comparative-constitutions-project/

13. Congressional Research Service (CRS). (2020). "Intelligence Community Support to Pandemic Preparedness and Response", *In Focus*, online at https://fas.org/sgp/crs/intel/IF11537.pdf

14. Easton, D. (1965a). *Political life as a system of behaviour. In D. Easton (Ed.). A framework for political analysis* (p. 23–34). Englewood Cliffs: Prentice-Hall.

15. Easton, D. (1965b). "Theory and behavioural research". In D. Easton (Ed.). A framework for political analysis (p. 1–22). Englewood Cliffs: Prentice-Hall.

16. Eiran, Ehud. (2020). 'Israel: Politics and Identity in Coronavirus times', in *The COVID-19 Pandemic in the Middle East and North Africa,* POMEP Studies 39, online at https://www.researchgate.net/publication/ 340793965_ Israel_Politics_and_Identity_in_Coronavirus_times/link/5e9e171b4585150839ef39da/download

17. European Commission. (2021). Horizon Europe Strategic Plan (2021 – 2024), 1st ed., Luxembourg: Publications Office of the European Union, 2021 doi:10.2777/083753

18. European Parliament (EP). (2021). *Foreign interference in democracies. Understanding the threat, and evolving responses*, *Briefing*, online at https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652082/EPRS_BRI(2020)652082_EN.pdf

19. Five Eyes Intelligence Oversight and Review Council (FIORC). (2017). *Charter of the Five Eyes Intelligence Oversight and Review Council*,

online at https://www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf

20. Foerster von, Heinz. (1960). "On Self-Organizing Systems and Their Environments," in Marshall C. Yovits and Scott Cameron, eds., Self-Organizing Systems (Oxford).

21. Foerster, H. V. (1979). "Cybernetics of cybernetics'. In K. Krippendorff (Ed.), Communication and control in society (p. 5–8). New York: Gordon and Breach.

22. Gentry, John A. (2020). "The New Politicization of the U.S. Intelligence Community", *International Journal of Intelligence and CounterIntelligence*, 33:4, 639-665, DOI: 10.1080/08850607.2020.1783134

23. Georgescu-Roegen, N. (1975). "Energy and Economic Myths', *Southern Economic Journal*, Vol. 41, No. 3, p. 347-381, online at http://www.uvm.edu/~jfarley/EEseminar/readings/energy%20myths.pdf

24. International Accounting Standards (IAS), online at https://www.iasplus.com/en/standards/

25. Kahana, Ephraim. (2021). "Intelligence Against COVID-19: Israeli Case Study", *International Journal of Intelligence and CounterIntelligence*, 34:2, p. 259-266, DOI: 10.1080/08850607.2020.1783620

26. Kerke van de, T. W. and Hijzen, C. W. (2021). "Secrecy, evidence, and fear: exploring the construction of intelligence power with Actor-Network Theory (ANT)", *Intelligence and National Security*, 36: 4, 527-540, DOI: 10.1080/02684527.2021.1893074

27. Kirzner, I., M. (2009). "The Alert and Creative Entrepreneur: A Clarification," Small Business Economics 32(2):145-152, online at DOI:10.1007/s11187-008-9153-7

28. Knodt, E., M. (1995). Foreward, in N. Luhmann, *Social Systems*. Stanford, CA: Stanford University Press.

29. Laslo, Alexander, Krippner, Stanley. (1998). *Chapter 3 – Systems Theories: Their Origins, Foundations, and development, Advances in psychology*, p. 47-74, DOI: 10.1016/S0166-4115(98)80017-4

30. Legrand, T. (2019). "Sovereignty renewed: Trans-governmental Policy Networks and the Global-Local Dilemma", in The *Oxford Handbook of Global Policy and Transnational Administration*, eds. Diane Stone, Kim Moloney, pp 200-222, online at https://books.google.com.au/books?id=Ex6DDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

31. Legrand, T. (2020). "From Insularity to Exteriority: How the Anglo sphere is Shaping Global Governance, in Understanding the Five Eyes", *Conference proceedings,* Centre for International Policy Studies, uOttawa, online at https://osf.io/k35pw/?show=revision

32. Leyen von der, Ursula. (2019). *A Union that strives for more. My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024*, online at https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

33. Luhmann, N. (1995) *Social Systems*, translated by J. Bednarz and D. Beacker, Stanford University Press, Stanford, CA.

34. Luhmann, N. (2000). *Die Politik der Gesellschaft*, Frankfurt am Main: Suhrkamp.

35. Malthus, Thomas, Robert. (1998). "An Essay on the Principle of Population, 1998", Electronic Scholarly Publishing Project, online at http://www.esp.org/books/malthus/population/malthus.pdf

36. Martin-Breen, P. and Anderies, J. M. (2011). *Resilience: A Literature Review*, September 18, online at https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/3692

37. Mathiesen, J., Mitarai, N., Sneppen, K., and Trusina, A. (2011). *Ecosystems with Mutually Exclusive Interactions Self-Organize to a State of High Diversity*, Phys. Rev. Lett., 107/8, online at https://doi.org/10.1103/PhysRevLett.107.188101

38. Maupertuis principle. V.V. Rumyantsev (originator), *Encyclopaedia of Mathematics.*, online at http://www.encyclopediaofmath.org/index.php?title=Maupertuis_principle&oldid=17452

39. McPhee, Justin T. (2020). *Spinning the Secrets of State: Politics and Intelligence in Australia,* Melbourne: Monash University Publishing, 2020.

40. Mele, Cristina; Pels, Jacqueline; Polese, Francesco. (2010). *A Brief Review of Systems Theories and Their Managerial Applications*. Service Science 2(1-2):126-135, online at: https://doi.org/10.1287/serv.2.1_2.126

41. National Intelligence Council (NIC). (2012). *Global Trends 2030: Alternative Worlds*, online at https://www.dni.gov/files/documents/GlobalTrends_2030.pdf

42. National Intelligence Council (NIC). (2021). *Foreign Threats to the 2020 US Federal Election*, declassified version of a report provided to the President, online at https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

43. Oneaşcă, I. (2018). *The European Social Model – Transformations needed in the light of international competitiveness and enlargement towards Southeast Europe* (Doctoral dissertation, Romanian Academy, in Romanian). Bucharest.

44. OECD. (2015 c). *Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development*, The

Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, Paris, *DOI: http://dx.doi.org/10.1787/9789264239012-en*

45. Office for National Statistics (ONS). (2018). *Household satellite account*, UK: 2015 and 2016, online at https://www.ons.gov.uk/economy/nationalaccounts/satelliteaccounts/articles/householdsatelliteaccounts/2015and2016estimates

46. Parsons, Talcott. (1965). *Il Sistema Sociale*. Torino Edizioni: Comunità**.**

47. Petersen, Karen Lund. (2019). "Three concepts of intelligence communication: awareness, advice or co-production?", *Intelligence and National Security*, 34:3, 317-328, DOI:10.1080/02684527.2019.1553371

48. Petersen, K. L. and Tjalve, V. S. (2018). "Intelligence expertise in the age of information sharing: public–private 'collection' and its challenges to democratic control and accountability", *Intelligence and National Security*, 33:1, 21-35, DOI: 10.1080/02684527.2017.1316956

49. Petersen, K. L. and Rønn, K. V. (2019). "Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society", *Intelligence and National Security*, 34:3, 311-316, DOI: 10.1080/02684527.2019.1553365

50. Piketty, Thomas. (2014). *Capital in the Twenty-First Century, Translated by Arthur Goldhammer, The Belknap Press of Harvard University Press*, online at https://dowbor.org/blog/wp-content/uploads/2014/06/14Thomas-Piketty.pdf

51. Stichweh**,** Rudolf**.** (2011). **"**Systems Theory"**.** International Encyclopaedia of Political Science**.** Edited by Bertrand Badie, Dirk Berg-Schlosser and Leonardo Morlino, DOI:http://dx.doi.org/10.4135/9781412994163

52. Thelen, E., & Smith, L. (2006)*. "*Dynamic Systems Theories', in *Handbook of Child Psychology, Theoretical Models of Human Development,* 6th Edition, eds. William Damon, Richard M. Lerner, p. 258-312.

53. UNCTAD (United Nations Conference on Trade and Development). (2020). *Technology and Innovation Report 2021*, UN, Geneva.

54. UNDP and MBRF (Mohammed Bin Rashid Al Maktoum Knowledge Foundation). (2020). *Global Knowledge Index*, online at https://www.undp.org/content/undp/en/home/librarypage/capacity-building/Global-Knowledge-Index-2020.html

55. UNESCO-UIS. (2014). *ISCED Fields of Education and Training 2013 (ISCED-F 2013),* UNESCO, Paris.

56. United Nation, DESA. (2019). *World Population Prospects 2019*, online at https://population.un.org/wpp/Population Division

57. United Nation, DESA. (2020). *World Social Report 2020 Inequality in a Rapidly Changing World*, UN 2020, online at https://www.un.org

58. UNODC (United Nations Office on Drugs and Crime), (2011). *Criminal Intelligence. Manual for Analysts. UN*, online at https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

59. U.S. Department of Justice (USDJ). (2019). *III Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller*, online at https://www.justice.gov/archives/sco/file/1373816/download

60. US PUBLIC LAW 108–458 – DEC. 17. (2004). *Intelligence reform and terrorism prevention act of 2004*, online at https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf

61. Wendt, A. (1992). "Anarchy is what States Make of it: The Social Construction of Power Politics". *International Organization, 46*(2), 391-425, online at http://www.jstor.org/stable/2706858

62. Wheaton, Kristan J.; Beerbower, Michael T. (2006). "Towards a New Definition of Intelligence", vol 17, *Stanford Law & Policy Review* 319 (2006), https://law.stanford.edu/publications/towards-new-definition-intelligence/

63. White House. (2019). *Executive Order 13859 of February 11, 2019*, online at https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

64. White House. (2021). "Interim National Security Strategic Guidance", The White House, Washington, online at https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

65. Wigell, Mikael. (2021). "Democratic Deterrence: How to Dissuade Hybrid Interference", *The Washington Quarterly*, vol. 44, pp. 49-67, doi: 10.1080/0163660X.2021.1893027

66. World Bank. (2021). *World Development Report 2021: Data for Better Lives.* Washington, DC: World Bank. Doi: 10.1596/978-1-4648-1600-0.

IMPROVING INTELLIGENCE TRANSPARENCY: THE JOINT VENTURE OF BUILDING AN INITIAL FRAMEWORK

Gabriela CONTU*

Abstract:

In the contemporary period, especially in the last three decades, transparency, openness and access to information have fallen into a new era of interest for numerous actors playing in the societal democratic arena – citizens, organizations, the private sector, governments, media, politicians, international partners and so on. A paradox of transparency should be its presence in the intelligence field – born and raised on a strong basis of secrecy and conspiracy. While questioning what intelligence transparency is or, how we like to call it – "intelligence in plain sight", we discovered the inexistence of a public, academic or institutional framework defining the topic.

Therefore, this article aims at taking the first steps into this direction, by defining a couple of constants and variables, essential parties and indicators which should be comprised into a strategic joint venture, setting out to develop a framework for the practice of intelligence transparency. Also, this article underlines the need for liaison between these factors, meant to balance between the two oxymoronic adjectives – secretive and transparent. The analysis starts with a picture of how transparency looks like for governments – whether they are open or not, and it goes on with a legal perspective, only to end by catching the few elements surrounding the intelligence transparency topic. The main contribution of this article is that it overwhelmingly underlines the gap in both academic and administrative literature for a framework for intelligence transparency.

Keywords: *transparency, secret, intelligence, legal, framework, joint-venture.*

* PhD Student, National School of Political Science and Public Administration, email: contu.gabriela.19d@student.comunicare.ro. An extended version of this article will be found in the PhD thesis in communication studies which will be defended at National School of Political Science and Public Administration.

Introduction

Is silence speaking? Is silence a tool for efficiency? Is silence still the best solution for intelligence agencies and services? This paper emerged from a paradox present in the public sphere, namely the silence of an intelligence community set in place in an environment characterized by an abundance of communication and openness.

Intelligence services "have become a social constant" (Postelnicu, 2012) and not a state extravagance and bear the stigmata of secrecy, and one may even say that they suffer from some kind of disease, a "maladie", "*mal-à-dire*", meaning that, in comparison to other state institutions, intelligence services are rather inclined to silence and have a *difficulty to communicate*. In this paper we aim to connect dots, so that we can come up with an initial framework for improving intelligence transparency.

In this attempt, we looked at the concept of transparency from its emergence in the governmental field, as a concept, as a practice, from a holistic perspective which includes legal aspects, risks and advantages, role and functions, as well as forms of manifestation. Also, we included a legal perspective on intelligence transparency in relation with the oversight bodies, which led to an almost unanimous perspective that there should be zero secret in this interaction and, implicitly, 100% transparency.

Building this kind of background, of a broader context, help us narrow the issues to our topic of interest, which is intelligence transparency. Our purpose was to identify the relations that connect the dots in a network of constants and variables capable of offering transparency in the intelligence field, which is ultimately defined as a framework. Within this framework, our analysis and projection brought together actors, stakeholders, standards, processes, but also contributors who have a leading role in developing knowledge and fostering understanding of the intelligence field and activity.

The concept of transparency

The concept of transparency is widely spread and often encountered and used worldwide, in connection with multiple actors:

from governmental institutions and non-governmental organizations, to academic topics and scientific research.

The concept of transparency was subject to academic literature, viewed through several lenses, focusing on its constituent elements, with well-established roles, rather than identifying comprehensive definitions. Following our analysis, we have established that, within the academic community, there has not been an agreement regarding a unanimously accepted definition of the concept of transparency.

On the one hand, while putting aside the concept and taking on the idea of transparency, available to all, a definition accessible to any individual who is not concerned with a fundamental evolution of the concept, in a given field or context, we looked at existing definitions in the Cambridge Dictionary (2020), where we identified two meanings that can be associated with the concept of transparency. The first meaning is "see through", which defines transparency as the ease of seeing through – "easy to read", which makes an existing subject more accessible, easier to understand, easier to approach. The second meaning is that of "open", which defines transparency as the quality of being open and without secrets. Another approach presented as a peculiarity with respect to official public administrations activities or any other organizational related topics, adds an essential element to the transparency equation, namely trust. Thus, transparency is defined as a situation in which financial or organizational activities are conducted openly, without secrecy, so that individuals can trust that they are fairly and equitably treated.

On the other hand, the fundamental approach to transparency, through academic study, reveals an impossibility to define the concept of transparency unanimously, due to its complexity and wide range of topics, areas, levels where transparency has a direct or indirect impact, functional or operational. With respect to the named diversity of fields, Ball (2009) refers to non-governmental or supranational organizations, to the field of international relations, to non-profit institutions and activities, to public policy-making processes or to the academic literature on public administration.

Continuing on the study of fields impacted by transparency, we found that the variety stated by Carolyn Ball was confirmed and

completed by Stiglitz (2002) who talks about the fact that, at the academic level, the concept of transparency has been approached in studies belonging to multiple fields, such as negotiation theory, international security, and administrative efficiency.

We can ascertain that there are several actors involved in the practice and theory of transparency and that there is a widespread interest in the concept, but we have come to believe that this is an actual double-edged sword, since the variety of areas in which transparency has a functional and operational impact leads to an impossibility in identifying an unanimously accepted definition. This initial assumption was confirmed by a number of researchers, who reinforce the idea that the lack of a definition is due to the complexity of the concept and the diversity of areas on which it has a significant impact (Relly & Sabharwal, 2009). Also, Florini (2007) argued regarding a specific type of transparency (government transparency) that a single definition has not yet been accepted neither by the academic community, nor by the practitioner's branch. The perceived cause at that time was the lack of understanding of the concept of transparency, which led to the difficulty of operationalizing and defining it (Grigorescu, 2003; La Porte, Demchak, & De Jong, 2002).

We can identify in the literature partial definitions, or rather definitions limited to the field where there is an established practice of transparency, setting fractioned frameworks of transparency roles, functions, contributions to the efficiency or effectiveness of a process or activity, or, conversely, of negative aspects due to a lack of transparency.

While keeping in mind the lack of a unanimous definition, the interest in the present article focuses on the relevant roles of transparency in given contexts and systems, rather than finding or building an explicit and singular definition, given the fact that we are mostly interested in the specific field of intelligence agencies and services.

Three-dimensional format: purpose – implementation – evaluation

The elements that constitute a process of transparency, in a three-dimensional format comprised of purpose – implementation – evaluation, are those that we will further identify, by exploring several areas, following on the role of transparency in their development.

In association with the public administration, Grigorescu (2003, p. 643-667) mentions that transparency is associated with "good governance", as a general principle, which leads to an increased difficulty in identifying a correct, applicable and specific operationalization of the concept, but defines a clear relationship between the governance process and the need for transparency.

While domains such as management or the administrative areas started to look for ways to increase their efficiency, transparency has emerged as a result of the need for a tool to help combat systemic development failures and counter democratic deficiencies (McGee & Gaventa, 2010). Researchers and practitioners who promote democracy, associate transparency, following the wave of democratization that took place in the twentieth century, directly with the need for control, specific to a modern, contemporary democratic system. Basically, democracies are required to "deliver the public good", and this action must be subject to new forms and tools of public control. Traditional forms of democratic control, involving only actions by the state towards its own institutions are considered to be outdated and increasingly insufficient. Thus, the need arose for multi-lateral control exercised both by public bodies, as well as by citizens – as an additional measure to those led by state institutions, designed to ensure ancillary, complementary supervision (Ball, 2009). Practically, transparency becomes the tool that provides the new control actors with the necessary information to follow the correctness of the government apparatus.

We can thus appreciate that transparency is closely linked to the control activity, as a complementary tool available to other actors than the institutional, traditional ones. After the mid-1970s, we can speak of a revolution, a reform of the public control forms, as traditional standards of control were systematically developed and strengthened,

so that the control activity became a system in itself and in its own right (Power, 1999). This is specific to the development of the contemporary society, which can be defined as an "audit society" or a "performance society" (Ball, 2012). The performance involves an actor who "performs", but also one or more of them who watch and evaluate what is available, open and made accessible to them.

The relationship between institutional actors and the public sphere was addressed by the Institute for Public Policy Research (2001) which discusses the public-private partnership (PPP) and introduces the idea of hybrid control, meant to support its performance. The basic principles proposed for the success of such a partnership are: transparency, clarity of roles and the ability to adapt to the citizens' needs.

Carolyn Ball (2009), in an attempt to define transparency, has identified associations with three representative metaphors for the concept of transparency.

In the first metaphor, transparency is perceived as a public value highlighted by society for its role in combating corruption, therefore there is a direct association of transparency with control activity and democratic governance.

In the second metaphor, transparency is synonymous with openness (accessibility and availability of knowledge) to the decision-making processes of governmental and non-governmental institutions. This association translates into processes subsequent to transparency, such as encouraging openness towards the public sphere, increasing concerns about the relationship between privacy and secrecy with respect to processes that involve, under certain conditions, the right to brake, through various specific methods, citizens' privacy (secrecy versus privacy).

In the third metaphor, transparency is perceived as a complex tool of good governance, used in various programs, policies, organizations at the state level. Within these systems, transparency is joined by other characteristics or features that ensure the success of a process, activities, program, and policies etc., which fall under the authority of decision makers. The related, complementary and interconnected characteristics are: transparency, control, efficiency and effectiveness. The most relevant aspects lie in the fact that they have a

significant impact, at organizational and structural level, being associated both with macro processes such as policy development and micro-processes being presented in the day-to-day activity of government employees.

Ball (2009), in his extensive analysis of transparency, concludes that this has become an unofficial mandate issued by the general public and more and more often a legal mandate.

The concept of legal mandate translates into the obligations of public administrations to grant access, in an organized, systemic and intentional way, to certain categories of information, the knowing of which is, in fact, a citizen's right. The existence of a balance and a coherent relationship between the legislative and executive systems is unequivocally necessary in a democratic state. The existence of such a functional system makes it impossible for one of the two branches to exercise a dominant control or influence over the other and could represent one of the main pillars in the prevention of possible abuses conducted by representatives of public institutions, including security and intelligence services.

Although democratic systems have been marked by traditional forms of administration, nowadays across the public sphere the clearly defined format and concept of control was intertwined with the complementary presence of transparency. Thus, Karp (2005) or former US President Barack Obama (2006) argued that, in the processes of democratic or organizational optimization, we started from the idea of "extended control" (greater accountability), only to reach a system based on balance and efficiency due to the relation between control and transparency.

Recent reports call for transparency in close connection to human rights and freedoms, based on a private – public balanced relationship, in the case of activities of collection and management of individual and bulk data, but also interception of communications (Eskens et al., 2016). This perspective has been identified in the chronology of the literature in several works, being approached similarly by authors such as: H. Born (2004), P. Birkinshaw (2006), C. Ball (2009), J. Klaaren (2010).

Even if we cannot expose a singular definition of transparency, we have extracted from literature a series of constitutive elements (constants), common to the idea of "transparent" and the concept of "transparency", which refer with predilection to the institutional, governmental architecture. These are representative of this paper, especially in terms of setting transparency roles in the functional and operational architecture of a modern democratic state. Thus, we can conclude the following about transparency:

- it is an organized, systematic process of communication;
- it is not specific to a field, but is approached and practiced multi and inter-disciplinary;
- it is an indicator of a democratic system, encouraging "good governance";
- it has a particularly important role to play in preventing and combating corruption;
- it involves public exposure and thus allows monitoring of the internal activity of organizations or institutions;
- it contributes, but is not limited to encouraging external control, to increasing an organization's credibility and to building a relationship of trust;
- it encourages access to the information, by high availability for all those actors who wish to be part of the complementary monitoring and control system;
- it lies between an unofficial mandate and a legal obligation.

Summarizing once again the approaches to transparency, the most important key words, the lack of which would render a discourse of transparency incomplete, are: good governance, democratic control, fight against corruption, unofficial mandate, legal obligation, trust.

Pin-pointing the emergence and evolutions of government transparency

The emergence of a globally-extended concept of government transparency is closely linked to a number of intrinsic but also extrinsic areas of government architecture, such as: the growth and internationalization of the media, the technological boom, the diversification of national security issues, the third wave of democratization post-Cold War (Finel & Lord, 2000, p. 3-5; Lord, 2006).

A preparatory legal perspective

And yet, which feature or field best defines the origin of transparency? Synonymy with good practice? Legislative obligation? Voluntary responsible behaviour of institutional actors? The manipulation tool that mimics openness through selective transparency? While some of the questions and options presented are predominantly subjective, one of them has been identified as an emerging source of transparency, namely the legal component. Referring to the legal norms and provisions associated to transparency, they began to rise in the 1970s and allowing citizens and especially the media to access to public information, mainly regarding the activity of the American public administration. Ball (2009) argues about this kind of provisions that "they created transparency".

However, we consider this conclusion to be a rather general one, with which we do not agree, as it relates strictly to the time of the 1970s, and due nuance is needed. Indeed, that period was marked by the emergence of legislative provisions on access to information (Freedom of Information Act – FOIA – 1966 – 1974, Whistle blower Protection Act – 1989, Sunshine in Government Act – 1976 etc.), which led the way to transparency through incipient forms, to the increased availability of information of public interest to the public sphere and media, to the education of the population to act in the sense of access to information, disclosure of abusive activities. We consider these to be only a starter, a catalyst, a trigger of a series reaction.

Other normative acts that created premises for the implementation and development of transparency were: Columbia (1985) – Law on the publicity of official acts and documents; Hungary (1992) – Law LXIII on the protection of personal data and access to data of public interest; Bosnia and Herzegovina (2000) – Law on free access to information, Romania (2001) – Law on free access to information of public interest etc. Land marking in 2017, worldwide, there were 119 countries that have adopted legal regulations on free access to information (Alphabetical and Chronological lists of countries with FOI regimes, 2007), and the full list can be found at www.freedominfo.org.

The Access Info Europe report (2006) has monitored, worldwide, acts on free access to information, concluding that, of the 65

pieces of legislation analysed in Europe and the US, 50 were aiming at providing extended access to information of public interest, highlighting that most developed democracies recognize this right (Access of Information: a Fundamental Right, a Universal Standard, 2006, p. 1).

As presented above, most approaches to transparency do not define or detail the concept itself, but refer to transparency in different contexts, functionally defined – in which case transparency is mentioned as a tool or policy of good governance or thematic – areas where transparency is or would be required. In either case, the literature records the need for public administrations to disseminate information of public interest, the variation of their typologies being quite large – from regulatory and normative materials to raw materials used in different areas.

Since the 1990s, we can say that, globally, the frequency of legislation on free access to information has been unprecedented. This process has not only been supported by legislation, but by other actors, such as non-governmental organizations. Researchers have identified a chronological parallel process which is represented by inter-governmental relations and practices, which exercised pressure on states in order to assume and implement transparency norms and practices (Relly & Sabharwal, 2009).

Various researches have shown that government transparency is a moral duty (Liston-Heyes & Juillet, 2020) and is closely related to the professional integrity of the public system (Mishory, 2013).

Simultaneously, transparency has been highlighted as having a functional purpose with respect to public institutions, as it creates the premises for a culture based on public trust and confidence, while building on the informed presumption of innocence.

From a thematic perspective, referring to the governmental system as a whole, transparency has often been defined in relation to the phenomenon of corruption: transparency would be "an essential element of the basic approaches used by governments to promote public openness and reduce corruption" (Bertot, Jaeger, Grimes, 2011, p. 79). The same article details the risks of lack of transparency, the main categories of risks identified being associated with corrupt

behaviour and tendencies. There are three categories of risks resulted from the lack of transparency, namely social risks (hindering the development of social trust and public interest), administrative risks (encouraging opportunism and favouritism in the allocation of physical or information resources) and managerial risks (reducing the efficiency of the public sector, by affecting partnerships with different actors).

According to the Corruption Perceptions Index, control and transparency are two key elements in reducing the degree of corruption at the state level, and directly and indirectly, in increasing public confidence in administration and governance (Liston-Heyes & Juillet, 2020).

Summarizing the approaches to government transparency, we can pin-point the time for emergence in the 1970s, through incipient, incomplete forms, and the beginning of the stage of conceptual coherence, in the 1990s.

Following up to nowadays, in the last decade, the most common framework for discussing government transparency is by changing parts of its DNA, a mutation from offline to online through eGovernment conception and tools.

eGovernment

When we talk about open government data – OGD – we can say that this is a trend, a movement that has created a niche for promoting availability of data, a transparency tool provided to public administrations, a niche that could be defined as eTransparency. The creation of online portals for data sets has met the major need of governments to promote transparency by publishing government-accessible data sets in an accessible environment to as many stakeholders as possible – such as online – that can be used for control activities on one hand by civil servants, and on the other hand by any actor interested in reusing and processing them for the purpose of social and economic development (Lourenço, 2015).

Researchers interested in this field raised two major concerns about the efficiency and complexity of this type of portals for online transparency: the first regarding their effectiveness in disseminating information and data to achieve the objectives of transparency and

control; the second regarding whether it is possible to actually evaluate the efficiency. Starting from the lack of assessments on the implementation of the principles of open governance, beyond the general idea of providing everything necessary and sufficient for control and transparency, the unanimous conclusion revealed the need for a set of specifications, rules, characteristics to define a pre-established evaluation framework.

The development of the portals started both from the need to be able to access collective, cumulative data, to the detriment of searches performed on the inhomogeneous pages of each public institution (with different structure, with different formats, with disparate and uneven types of information), to encourage public administrations to develop a strategy of transparency and extensive control and to generate a series of standards for publishing data of public interest (Lourenço, 2015).

In general, the two criteria taken into account for designing the architecture of such an online portal are the type of public entities (authorities) that will be engaged and the types of information that will be published. Globally, the main types of information in collective data set portals are performance indicators – budgetary, financial and data management. From this perspective, the question that arises is whether national security information that is likely to be part of the processes of transparency and construction of the security culture can or should be present in these types of portals, should be disseminated through other channels and tools to specific audiences or shouldn't be published at all. Even more, from this article's perspective, we are interested in the cumulus of actors and indictors that could provide a framework for evaluating the above-mentioned issue.

Last but not least, what is particularly important about eTransparency is that the literature has mostly confirmed two hypothesis: the information provided on an institution's own website is a proxy for the level of transparency of that entity; the second conclusion is a quantitative one, namely that the dissemination of an enormous amount of data and information does not equate to increasing the level of transparency and does not necessarily and unequivocally facilitate the control activity (Lourenço, 2015).

Advantages of transparency and the risks of its lack

Before going forward approaching transparency related to the intelligence field and activities, we will present a series of general advantages and risks related to the use and lack of transparency, in order to provide an initial framework of analysis, which can be extended or reduced while applying it to the intelligence domain.

Arguing the benefits of transparency, studies conducted with respect to states that have implemented transparency measures across the public sector have shown a tendency to produce more information of public interest than other similar governments and a predisposition to increased and more complete dissemination of this information to civil society than those that do not have an institutionalized practice and tradition of transparency (Lord, 2006).

While looking at public stakeholders and promoters of transparency, we have identified a pioneer in defining and promoting institutional transparency as an instrument of good governance. Namely, we are presenting the work of Barack Obama, who issued at the beginning of his term as President of the United States of America, through the institution of the Presidential Administration, a Memorandum on Transparency and Open Governance for the heads of executive departments and agencies, followed by a governmental progress report, in which transparency has been defined among the core values of the Obama administration, along with public participation in the act of governing and intra-governmental collaboration. According to the report (2009, p. 1), the governmental agencies and departments have a duty to provide citizens with information on the work that is carried out, in order to provide sufficient and necessary elements for possible accountability (not referring to the control activity).

The Obama Administration initiative has started a trend and a good practice regarding the principles and advantages of implementing transparency across the public sector, aspects arising from the concern and debate in the public space and in the academic environment that followed.

On the one hand, transparency, as part of the foundation of a good governance framework, is intertwined with a wide range of

principles, such as effectiveness, efficiency, accountability, responsiveness and integrity. On the other hand, while talking about the public sector as a whole, transparency is mainly introducing risks by its nonexistence, risks that are visible and cannot be ignored on a longer term. At the social level, the lack of transparency allows the creation of mental scenarios across the population, based on non-objective information, incorrect and/or incomplete. Typical sources of such scenarios are cultural customs and beliefs, the result of various experiences and narratives created and made available in the public space by stakeholders, other than the one belonging to the government and public administration (media, bloggers, vloggers, social media groups and influencing public profiles etc.). Also, the lack of transparency, in opposition to its presence, creates premises for reducing social trust and confidence in the public administration as a whole and also at an individual level – as a result of apparent secrecy. Also, whether we talk about countries where the level of trust and confidence is already very low, the lack of transparency is one of the most counter-productive measures that stay in the way of developing and increasing it in a healthy manner.

The lack of transparency is also a premise for opportunism, and the main categories of risks identified are associated with corrupt behaviour and trends. In addition to the social risks presented earlier, the literature has also identified administrative risks (encouraging opportunism and favouritism in the allocation of physical or information resources) and managerial risks (reducing the efficiency of the public sector, by affecting partnerships with different actors) (Bertot, Jaeger, Grimes, 2011, p. 80).

Intelligence transparency or intelligence in plain sight

The concept of intelligence has been defined by several authors throughout the twentieth and twenty-first centuries, but the classic meaning is that presented by the father of the intelligence field, Sherman Kent, who established a multidimensional definition, through three elements: activity, process and knowledge (Kent, 1966, p. 7). We note the use of the term knowledge in connection with intelligence which is more than information, it is custom made knowledge (Krizan,

1999), through a complex process of continuous collection, verification and analysis of information, which allows us to understand the problem or situation in actionable terms (Krizan, 1999, p. 7).

In this paper we are interested in intelligence activities conducted by state institutions with clear legal responsibility in the field – namely intelligence services and agencies. These are the main actors we focus on, followed by the other stakeholders who are present and notable in the public sphere – oversight bodies, media, and civil society.

The intelligence services work ex officio with classified intelligence and documents, which fall under the concept of secrecy, as stated by an intelligence practitioner, "the world of intelligence, traditionally closed, specialized in knowing and keeping secrets" (Westerman, 2019, p. 31).

While considering the fact that intelligence agencies are part of the governmental apparatus, but at the same time have particularities with respect to their public statements, communication, oversight and control information, in this paper we focus on the relation between secrecy and transparency, for this is, the turning point that differentiates governmental transparency from intelligence transparency. Over time, various policies and measures have been developed to reduce the distance between the intelligence services and the rest of the government apparatus, but it is expected that a perfect balance of control will not be achieved, given the inherent secrecy of business traditional executive ownership and control of intelligence activities by the secret services (Lester, 2015, p. 1-2).

When looking for a more clear connection between intelligence and secrecy we have identified that, while conducting its role in ensuring the national security of a state, the essential functions of intelligence are (Lowenthal, 2003, p. 2-5): early warning of strategic threats; making predictions and expertise on long-term security developments; providing information support and support in the decision-making process by state decision-makers and, occasionally, by other actors working in the field of state security (e.g. private actors managing critical infrastructures); maintaining the secrecy of national

security information, intelligence requirements, sources, methods and means.

Transparency in intelligence is a recurring topic both on the agenda of public opinion, of the legislative bodies, and of control and oversight committees in multiple states. Intelligence services view transparency rather as a negative and risky element than a positive trend specific to reform and modernization processes, leading to new forms of communication and control specific to democratic systems. Transparency is associated with a decrease in the efficiency of intelligence activities, as the nature of the intelligence services' activity is characterized by silent efficiency, and therefore by a high degree of secrecy. In consolidated democracies, a solution for the public-secret dichotomy has been identified, in strict compliance with legal provisions, democratic principles and by assuming the values that characterize the balance between transparency and effectiveness. In the US, one of the identified systemic solutions in achieving a balanced equation of transparency-secrecy has been to reduce corruption and increase control and oversight activity (Doorey, 2007).

We discussed Lowenthal's perspective (2003) on the functions of intelligence, the fourth being "maintaining the secrecy of national security information, intelligence requirements, sources, methods and means". The difficulty for intelligence services and agencies is to maintain a balance so that they can cultivate a climate of social trust, while not jeopardizing the security of their missions.

This taxonomy is particularly important from the perspective of openness to intelligence, as it could be a starting point for achieving standards of transparency, by establishing categories of data and information that are not intended to be made public – national security information, of intelligence requirements, sources, methods and means.

The literature highlights the need for a layered system of transparency measures, setting out the rules for the dissemination of information, based on clear policies, so that it does not depend on an arbitrary and unilateral decision of institutional decision-makers. The layered system is defined according to a number of constituent elements, such as the target audiences, specialized by their needs for transparency (oversight bodies, media, civil society – with special

attention to non-governmental organizations), the moment of communication or transparency, as well as the need to establish what can and cannot be made public – as a standard, in the form of a predefined list of information.

According to Eskens, van Daalen & van Eijk (2016), the layered transparency system can be characterized according to the following categories of elements and activities:

- informing the external actors involved or affected – individuals, national control bodies, civil society;
- ensuring an adequate level of openness to the intelligence activity, before, during and after the activity;
- making available that information, contexts, deliberations, statistics, operational data etc., which will not be disseminated publicly, for being classified.

The field and practice of national security is defined by the coordination and development of specific capabilities. Free access to information managed by actors directly involved in this field is subject to a limited level of expectation.

The expectations of citizens or actors involved or co-interested in the field of national security are defined by the development of the security culture. It should be noted, however, that expectations are not homogeneous and depend on the relationship between the specific actors with the intelligence regards. If the general public has a level of expectation related to their own needs and interests, institutional actors define a level of expectation that is rather regulated by legislation and procedures, given their roles in the government architecture.

In democracies, the so-called secret services – public institutions engaged in intelligence activities, oversight and transparency are key elements for the two present the reflection of the system in which they operate, while serving on one hand the individuals and on the other the democratic society (Spielmann, 2012). The author highlights the relationship between the operational requirements specific to national security and the need for instant audit, while conducting operations, as an asymmetric one, which can be balanced by transparency measures at the level of intelligence services. These measures are addressed both to

the general public and to bodies that generate formal oversight mechanisms.

Legal perspective on intelligence transparency towards oversight bodies

While considering different stakeholders of intelligence transparency, we have identified that one of the most important one is or should be the bodies which are mandated to exercise oversight on the intelligence agencies and services. From an emerging legal point of view with respect to the legal responsibilities of these bodies, they were adopted in the immediate vicinity of the 1970s, the zero moment of openness to transparency (Born, Johnson, & Leigh, 2005). Thus, these oversight bodies have been invested with the responsibility to:

- 1974 – USA – evaluate all national intelligence agencies, approve zero-level priorities, verify both the legality and efficiency of intelligence services, while having full access to the necessary information, regardless of classification level;
- 1984 – Canada – verify the legality and efficiency of intelligence services, having full access to the necessary information, regardless of classification level;
- 1994 – United Kingdom – audit budgetary, administrative and strategic aspects of MI5, MI6 and GCHQ, specifically those related to the efficiency of the services' activity, without involvement in assessing compliance with legality; access to the necessary information was provided, but not guaranteed when the subject had a very high degree of sensitivity;
- 1995 – Poland – verify the legality of the activity, budgetary, administrative and strategic aspects, without pursuing the efficiency of the services; access to necessary information was left to the "discretion" of intelligence agencies;
- 1995 – Norway – mainly verify the legality of the activity of intelligence services, including from the perspective of human rights, with full access to the necessary information, regardless of the level of classification.

The joint venture for improving intelligence transparency – a three-layered framework

Building on the above sections, this chapter aims at drawing a first set of criteria for designing a framework for improving the intelligence transparency practice, while taking into consideration all essential elements for this kind of joint venture, as presented in Figure 1.

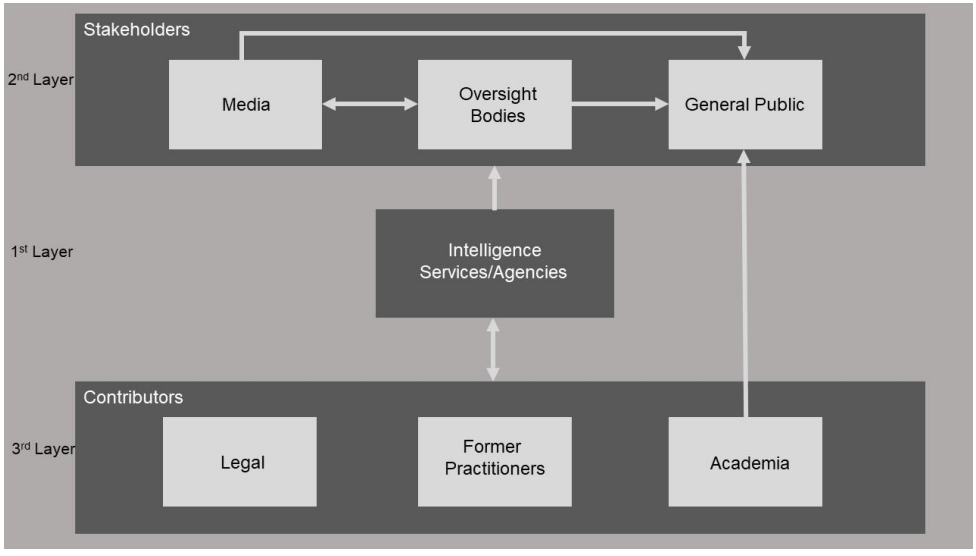


Figure 1: A three-layered framework
for improving intelligence transparency

The first layer

The first layer of this framework, the nucleus, is of course represented by the intelligence services and agencies. Their audiences should be comprised of all possible stakeholders, while the level of transparency should be layered depending on a series of standards. Leaning on the need to protect and hold a high level of security of their missions, the first standard for transparency that we propose is establishing and communicating categories of data and information that are not intended to be made public – national security information, intelligence requirements, sources, methods and means.

The second standard of transparency refers to the channel for display. While for specialized stakeholders there are pre-set roles that handle the transparency (e.g. for oversight bodies – top management, for media – public information office) there must be an open channel of communication, available to all direct and indirect stakeholders, at all times, and we propose as standard setting up the institution's own website (no matter the integration with other online platforms of eInitiatives), considering that the website is one of the best proxies for the level of transparency of a public entity.

Last, but not least, the third standard of transparency led and implemented by the intelligence community members is setting right-levelled classification of documents and information, so that it does not limit the access to public information without proper justifications.

The second layer

The second layer of relevant actors for this framework is represented by stakeholders. For an intelligence community, the main stakeholders that we are interested in are the oversight committees (for oversight purposes, but also for mediating the relation with the executive and legislative bodies), followed by the media and the general public.

We consider the highest level of openness and transparency should be directed towards the above-mentioned category of stakeholders, and by highest we refer, if possible, depending on the country, to having full access to the necessary information, for oversight involves knowledge, understanding and direct impact on the activity of intelligence bodies. Subsequent to the process of transparency, from intelligence agencies towards the oversight committees, and considering the highest level of access, these committees must perform transparency and communication acts toward the other stakeholders – media and civil society, presenting guarantees that they have accomplished the mandate they were given. The information should contain at least the annual number of closed sessions that took place for oversight or connected purposes, where there have been identifications of irregularities and whether measures of correction have been implemented (while protecting the secrecy of information, measures

etc.), whether the assessed institutions had available all needed resources to comply with their legal responsibilities and whether corrections are needed.

Media is a type of stakeholder that carries out two functions: receiver and giver. On one hand it is receiver of narratives from official actors and also from off-the-record sources, narratives which are being transformed and passed on to the general public. The role of media in this framework emerged from the fact that even if we were to ignore, it would still be there. Narratives are being produced and published every day and it is only up to intelligence service whether they provide their own, to be considered and integrated.

The general public is the beneficiary of the intelligence activities and a stakeholder found at the end of the narrative chain. The public mandate given to other responsible bodies except the general public from direct actions and oversight, but the right should still be in place, offered by transparency measure by the other actors from the arena. Making all public information available is a form providing the general public with the chance to perform unofficial oversight over the intelligence community members.

The third layer

The third layer of actors for this framework is represented by contributors. The contributors are those actors who can fill gaps with knowledge, understanding and legal background.

Knowledge and understanding of the intelligence system are of interest to all direct stakeholders, but also to indirect stakeholders, for processing public narratives. The contributors for filling these gaps are the academia, former practitioners (mostly involved in think-tanks and NGOs). On the other side, the legal context and background must be provided by the legislative branch of the state, as well as by the coordinator of the national intelligence community for each state, for a layered system of transparency measures who sets out the rules for the dissemination of information must be based on clear policies (legal provisions, standards, norms), so that transparency does not continue to depend on an arbitrary and unilateral decision of intelligence decision-makers.

Conclusions

We shall start the conclusions by presenting the limits of this research. On one hand it was generated from the lack of perspective of practitioners of "secret" and on the other hand from the fact that this research is in an incipient phase and only presented a basic scheme for a possible framework for improving the intelligence transparency practice, leaving the door open for further research, for further contribution from all stakeholders and from academia, as source of integrating knowledge and understanding of the intelligence in plain sight.

Even so, we believe that the proposed framework presents novelty in the field of intelligence transparency because it can be used on so many different levels. It can be used by the legislative branch to develop coherent provisions which can help lining up intelligence, in a safely manner, with other governmental agencies; it can be used by the oversight bodies to look at the way the results of their work are being communicated, or not, to the initiators of the mandate – the general public, it can be used by media to better know how to ask proper question and how the best recipients of their question are, it can be used by the general public to create buzz, to own up to their most-unguessable rights.

In addition, we believe that this paper represents a step in the process of filling the gap between the actors and stakeholders of the intelligence field, starting with the most important and relevant ones, while leaving enough space for introducing other constants and variables in the scheme and building a most complex framework, not for improving, but for definitively defining the practice of intelligence transparency.

References:

1. Ball, C. (2009). "What is transparency?", *Public Integrity*, 11(4), p. 293-308.

2. Ball, S. (2012). "Performativities and fabrications in the education economy: Towards the performative society?", *Australian Educational Researcher*, 27(2), p. 1-23.

3. Bertot, C. J., Jaeger, P. T., & Grimes, J. M. (2012). "Promoting transparency and accountability through ICTs, social media, and collaborative e-government". *Transforming Government: People, Process and Policy*, Vol. 6, no. 1, p. 78-91.

4. Birkinshaw, P. (2006). "Transparency as a Human Right", *Proceedings of the British Academy*, no. 135, p. 47-57.

5. Born, H. (2004). "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices", *Connections: The Quarterly Journal*, no. 03(4), p. 1-12.

6. Born, H., Johnson, L., & Leigh, I. (2005). *Who is watching the Spies? Establishing Intelligence Service Accountability*. Lincoln, Nebraska: Potomac Books.

7. Doorey, T., J., (2007), "Intelligence Secrecy and Transparency: Finding the Proper Balance from the War of Independence to the War on Terror", *Strategic Insights*, vol. 6, Issue 3.

8. Eskens, S., van Daalen, O., & van Eijk, N. (2016). "10 Standards for Oversight and Transparency of National Intelligence Services", *Journal of National Security Law & Policy*, no. 8(3), p. 553-594.

9. Finel, B., & Lord, K. (2000). *Power and Conflict in the Age of Transparency*. New York: Palgrave Macmillan US.

10. Florini, A. (2007). *The battle over transparency*, in A. Florini, (2007). *The right to know: Transparency for an open world* (p. 376). New York: Columbia University Press.

11. Grigorescu, A. (2003). "International organizations and government transparency: Linking the international development realms", *International Studies Quarterly*, no. 47 (4), p. 643-667.

12. Karp, J. (2005). "U.S. to Impose More Oversight on Lockheed Contract", *Wall Street Journal* (Eastern ed.): A2.

13. Kent, S. (1966). *Strategic Intelligence for American World Policy*. New Jersey: Princeton University Press.

14. Klaaren, J. (2010). *The human right to information and transparency*.

15. Krizan, L. (1999). "Intelligence Essentials for Everyone", *Joint Military Intelligence College.*

16. La Porte, T. M., Demchak, C. C., & De Jong, M. (2002). "Democracy and bureaucracy in the age of the Web – Empirical findings and theoretical speculations", *Administration & Society*, no. 34(4), p. 411-446.

17. Lester, G. (2015). *When Should State Secrets Stay Secret? Accountability, Democratic Governance and Intelligence*. Cambridge University Press.

18. Liston-Heyes, C., Juillet, L., (2020). *Burdens of transparency: An analysis of public sector internal auditing*. Institute of Internal Auditors, Ottawa.

19. Lord, K. M. (2006). *The Perils and Promise of Global Transparency*. Albani: University Press of New York.

20. Lourenço, R. P. (2015). "An analysis of open government portals: A perspective of transparency for accountability", *Government Information Quarterly*, no. 32, p. 323-332.

21. Lowenthal, M. (2003). *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press.

22. McGee, R., & Gaventa, J. (2010). "Synthesis report: Review of impact and effectiveness of transparency and accountability initiatives", Transparency & Accountability Initiative, Institute of Development Studies.

23. Mishory, E., (2013). *Clarifying Transparency: Transparency Relationships in Government Contracting*. Retrieved from SSRN: https://ssrn.com/abstract=2350020

24. Obama, B. (2006). "Does the Legislative Transparency and Accountability Act Provide Sufficient Reforms?", *Congressional Digest*, no. 85(5), p. 139–147.

25. Postelnicu, C. (2012). "Capacităţi instituţionale şi initiative asumate de realizare a securităţii. Serviciile de informaţii şi societatea civilă", *Revista Intelligence* – https://intelligence.sri.ro/capacitati-institutionale-si-initiative-asumate-de-realizare-securitatii-serviciile-de-informatii-si-societatea-civila/

26. Power, M. (2011). *The Audit Society: Rituals of Verification*. Oxford Scholarship Online.

27. Sabharwal, M., & Relly, J. E. (2009). "Perceptions of transparency of government policymaking: A cross-national study". *Government Information Quarterly*, no. 26 (2), p. 148-157.

28. Spielmann, K. (2012). "I Got Algorithm: Can There Be a Nate Silver in Intelligence?", *International Journal of Intelligence and Counter-Intelligence*, Volume 25, Issue 4.

29. Stiglitz, J. (2002). *Transparency in government*. The Right to Tell. Washington D. C.: World Bank.

30. Westerman, I., (2019). "Integrating Intelligence Practice and Scholarship: The Case of General Intelligence and Security Service of the Netherlands (AIVD)", *Romanian Intelligence Studies Review*, no. 21, p. 31-40. Retrieved from www.animv.ro

31. (2009). *Memorandum on Transparency and Open Government. Barak Obama Administration*, https://obamawhitehouse. archives.gov/the-press- office/transparency-and-open-government

32. (2006). *Access of Information: a Fundamental Right, a Universal Standard. Madrid: Access Info Europe*, accessed at https://www.access-info.org

33. (2007). *Alphabetical and Chronological lists of countries with FOI regimes*, accessed at http://www.freedominfo.org

34. (2020). Cambridge Dictionary

35. (2001). https://www.ippr.org

HISTORY AND MEMORY IN INTELLIGENCE

HISTORICAL PRECEDENT OF COOPERATION IN MATTERS OF INTELLIGENCE

Andrei FORTUNA*

Abstract:

In the contemporary security environment, characterized by the continuous dynamics of interdependence between the elements of national security systems, as well as the international ones – with similar institutions of other countries, the importance of integrated cooperation becomes increasingly influential, both in internal decision-making and in training the content of international relations. Of particular importance for the geographical structure (in a geopolitical, geo-economic and geostrategic aspect), is the level of economic and technological development of the states participating in this cooperation network, taking into account the advancing share of cyber, terrorist, extremist, criminal, etc. risks in contrast to the degree of development. Based on this consideration, the differences in the colours of political regimes will traditionally be of secondary importance to the pragmatic needs of the situation. Respectively, the cooperation criteria, in the perspective of its structure, remain unchanged, yielding only to the emergence of new content priorities. Developing from the specifics of the international security environment at all levels – regional, continental and global, taking into account the uninterrupted development of the transnational aspect of contemporary threats, the diversification of hostile forces and means of exerting influence in subversive forms – the changes become clearer. In order to prevent and counteract them, it is necessary to emphasize fundamental knowledge – a condition in which national and community intelligence authorities, at the institutional level of the European Union, strengthen their priority function of anticipating ensuring security through offensive actions, whose qualitative content will depend on the availability of excellently trained, motivated and remunerated human resources.

Keywords: *authorities, cooperation, coordination, institutional, intelligence, security.*

* PhD, "Bogdan, Intemeietorul Moldovei" National Intelligence and Security Institute, Republic of Moldova, e-mail: andreifor@gmail.com

Introduction

In spite of many obstacles, the common and permanent goal of special services cooperation, at the national or at the international level, has always been to identify, prevent and counteract dangers to interests of national security. This integrated formulation aims at establishing strategies and continuous transformations of contemporary security authorities, so as to avoid duplication, overlap or unfair competition at the institutional level, inevitably followed by unjustified resource costs. This article aims to emphasize cooperation efforts and the importance of outcome for security and intelligence authorities in the context of a constantly changing environment in terms of risks and threats. To this end, the specific regulatory framework for cooperation between special services has been examined, as well as the actions taken to develop this cooperation at the national and international level.

With the adoption in 1998 of the Concept of National Security of the Republic of Moldova, the objectives of ensuring national security were clearly mentioned, both on the territory of the country and abroad. The intelligence activity, as an element of ensuring the national security of the Republic of Moldova, is placed on the list of other institutional activities – political, economic, diplomatic, etc. International cooperation, as a tool to ensure and strengthen national security, is represented by a separate chapter. (*Concepția securității naționale a Republicii Moldova,* 2008)

European standards and practices are stipulated, the document being limited to this universal participation in international efforts aimed at managing contemporary threats and challenges, such as "Fighting terrorism". Tangentially, the respective issue can be observed in the other compartments, not included in the aforementioned list, but their importance is secondary in the context of cooperation on this specific field, depending on the commitments assumed. (*Strategia securității naționale a Republicii Moldova*, 2011)

International cooperation, at the bilateral or multilateral level, in the field of intelligence and counter-intelligence, is possible only if it is based on the unity of purpose, objectives and strategy, on the basis of information provided by the participating intelligence authorities. Their activity in such a format is determined by the particularities and

customs of the participating countries, by the way common interests are understood and formulated, by the differences in the levels of security culture in the countries they represent, by their ability to perceive the importance of special services. The need for the cooperation of intelligence authorities is determined by the following conditions:

1) The emergence of sources of international insecurity with historical, territorial, ethnic, religious, political, or ideological origins;

2) Risks and threats to the interests or national security of a state;

3) Dynamics of the level of danger of risk factors from an external opponent;

4) Radicalization of international terrorism;

5) Intensification of the information-media war, characterized as an uninterrupted process.

As an institutional phenomenon, cooperation between security agencies is aimed at coordinating, in an integrated manner, the activities carried out by the intelligence authorities of different countries and evaluating, in an integrated way, the information obtained concerning national security.

With a developed legal framework for inter-institutional cooperation in the field of intelligence, its establishment and consolidation has been a successful process for several reasons, taking into account that all intelligence authorities, without exception, are bureaucratic institutions with specific internal regulations, which always delay processes. Likewise, the existence of several services with overlapping responsibilities and roles affects efficiency and cooperation and leads to unfair competition or professional rivalry, able to reduce to zero the very meaning of inter-institutional cooperation, approved at the highest level of states. In order to develop and strengthen such cooperation at the international level, bilateral or multilateral cooperation protocols are established, which allow for the creation of various functional mechanisms, including for the operational exchange of the intelligence of common interest. The main communication tool in the cooperation process is the exchange of information, including through the creation of integrated communication networks.

This research defines the concept of security through cooperation. Cooperation in the intelligence area exceeds the classification according to the structural-quantitative criterion according to the levels of cooperation at bilateral and multilateral level, giving way to other approaches. Thus, such a format as the "Bern Club", which has been active since 1971 at the initiative of the USA, France, Germany, Belgium, Denmark, Great Britain and Switzerland, respectively, was created for the technical coordination of counter-terrorism cooperation (Troncotă and Blidaru, 2010). This structure currently brings together the heads of security services of the EU member states, providing the framework for informal thematic meetings on current issues that may threaten the common interests of the participating countries.

The next example, the Kilowatt Group, which has been active since 1977, brings together representatives of intelligence and security services from 15 EU countries: Belgium, Denmark, France, Germany, Ireland, Italy, Luxembourg, Spain, Sweden, the United Kingdom, Canada, Switzerland, Israel, Norway and the United States also on the subject of international terrorism. In the same context, the other thematic cooperation structures are highlighted, such as the Pompidou Group, the STAR Working Group (Ständige Arbeitsgruppe Rauschgift), the Vienna Club, the Mediterranean Club, the Safari Club or the NATO Special Committee (Troncotă and Blidaru, 2010, p. 3).

Taking into account the fact that in the list of member states of the respective structures there are, in most cases, with rare exceptions, the same states with founding status, it is important to highlight the existence of an informal network of operative exchanges of information, with a priority on related issues – asymmetric risks, such as international terrorism, organized crime, illegal migration. Obviously, this cooperation is rather a kind of strategic truce, conditioned by the existence of long-term risks with the impossibility of solving them based on their own resources.

The practice of informal cooperation, usually based on bilateral bases, is more frequent. Often, such cooperation takes place between Border States who shares a series of common interests. Contrary to these forms of cooperation, the policy of the participating states in this

field is carried out taking into account the priority of their own national interests to the detriment of the interests of the partners. There are several arguments that justify such approaches.

The protection of information sources is a principle strictly respected by all intelligence services without exception, as the most sensitive, important and vulnerable segment of intelligence activity in general. Moreover, as a rule, the exchange of evaluations and analyses has priority in relation to primary information, obtained directly from the first source, which again can put it at risk of uncontrolled development. At the same time, for example, the Romanian legislation does not exclude that, in well determined and substantiated situations, at the proposal of the director of the Romanian Foreign Intelligence Service (SIE), approved by the Supreme Council of National Defence (CSAT), intelligence human sources may be engaged in operations on cooperation actions with allied intelligence agencies (*Law* no. 1/1998).

The admission of this stipulation is based on secular experience in this professional field, references to which can be found, for example, in Chapter 12 of the Treaty on the Art of War, by describing, in particular, such a category of intelligence agent as an irreversible agent – person attracted in an intelligence, counter intelligence or disinformation operation, as a result of which it loses its quality of agent, by virtue of such conditions as the development of its real identity in the face of the enemy or the loss of life. (Sun Tzu, 2000, p. 110) The efficiency of cooperation demonstrates a pragmatic character, according to the reciprocity principle, according to which, the exchange of operative information is realized on the basis of a similar offer – immediate or perspective. For this reason, institutional cooperation between the special services of different countries with the attraction of human sources of information can be extremely costly, with the risk of reducing the importance and usefulness of the cooperation in question. This will condition the intensification of cooperation in the field of shared use of technical sources of information, convincingly argued for budgetary reasons, created on the basis of the costs of sophisticated technologies.

For instance, the Helios 1 program is an eloquent example of effective cooperation in this field. This program, which involves France

(78.9%), Italy (14.1%) and Spain (7%), is aimed at producing two military optical satellites – Helios 1A and 1B, launched into orbit on July 7, 1995, and respectively December 3, 1999 (Troncotă and Blidaru, 2010, p. 7). More than 30 French, Spanish and Italian companies have contributed to the realization of the Helios 1 program. In the summer of 2005, the governments of Belgium and Austria offered the establishment of an EU intelligence service, following the CIA model, with responsibilities in the field of preventing and combating terrorism. However, the proposal was rejected, as it was obvious that the main European powers were not willing to exchange information with all 25 EU member countries. The main opponents of setting up a European intelligence organization are the "Big Five" – the United Kingdom, Germany, France, Italy and Spain, which have strong intelligence services as well as the Netherlands and Sweden which cooperate within SITCEN, not being interested in revolutionizing the current EU intelligence cooperation system (Troncotă and Blidaru, 2010).

Moreover, due to the conservative nature of intelligence agencies and the bureaucracy specific of this type of organizations, the intelligence services generally consider that the only intelligence and analysis on which they can rely 100% is that of their own; to this national pride is added. In addition, the national intelligence communities of the EU member states are organized differently, in many cases a service in one state having no equivalent in another. To be successful, any cooperation should be based on mutual trust; in the field of intelligence, this concept has a relative value, the establishment of relationships based on trust requires a long time. The process of setting up a European intelligence agency would take place in several stages.

The financing of the services, the results of the operations and their content refer to the category of classified information, thus, there is a need to connect the legislation of the states participating in this cooperation in the field of intelligence. Therefore, the institutional cooperation of the special services of different states is not subject to extensive debate in society (in the media) or at parliamentary level, unlike other agreements and treaties. The retention of such a degree of secrecy by the governments of the participating countries has consistently led to contradictions with the principles of democracy, and

this issue remains open. Thus, due to the impossibility of exercising full control over the services, especially, in the process of their cooperation, is an advantage for them. Detailed knowledge of the strategic situation, possible scenarios for its development, dangers and threats, options for response actions create premises for: defining national interests, developing the national security policy, planning the tasks of intelligence services.

The fast development of the international situation stimulates the search for information on national security issues which the governments of different countries are facing nowadays. With the growing predominance of internal interethnic factors, national security is becoming even more dependent on both regional and global stability and the balance of reciprocity of international support from countries participating in intelligence cooperation. As geographical remoteness cannot guarantee the necessary security against contemporary risks and threats, cooperation in the field of intelligence between states must integrate its potential in this regard. At the same time, there is a need to increasingly focus intelligence services on conflict prevention, management and prompt response to crises. The range of tasks assigned to intelligence services today is more complex and dynamic compared to previous periods.

From a historical point of view, states always had a tendency to support each other, when they shared common interests of intelligence and had common points of connection, most often that type of cooperation was mutually beneficial. Even in cases where the interests of different countries do not completely coincide, their special services cooperate in conditions where the unilateral settlement of certain security objectives is impossible. Mutual cooperation usually includes exchanges of information on topics of common interest. Such kind of cooperation may take a long time, provided that both parties strictly comply with the agreements underlying such cooperation. Its essence is that the sources and details of the information provided by the partner will be protected according to their degree of secrecy and will not be transferred to a third party.

Although countries with insufficient intelligence resources may not offer opportunities for cooperation, comparable to those of

superintendent intelligence authorities, they may condition reciprocity through other opportunities. In some cases, such countries provide geographical or other access, which would not be possible otherwise. In other cases, small country intelligence authorities may provide expertise and other types of support, which would be difficult and more costly for their counterparts in the list of superpowers. In the information age, when such geopolitical or geo-economic attributes of the state, such as territorial expansion, population size or the availability of certain raw material platforms, have decreased in importance, giving way to the development of political culture, managerial technologies and sector development, cooperation between the intelligence services becomes inevitable.

In addition to the access and opportunities in the possession of the state, there is also the extraordinary advantage of attracting new allies based on honest relationships, which can be used in situations of crisis or other difficult times. The intelligence authorities demonstrate their high utility in the process of strengthening such relations on the basis of institutional cooperation agreements in the intelligence area – a process which is constantly expanding. There are currently no special services, able to act absolutely independently and efficiently in any part of the world, which is an important reason for maintaining and developing international cooperation in this field. There are a number of international forums, recognized in different proportions.

New contemporary dangers and threats, the expansion of international intervention and multinational peacekeeping activities explain the rapid increase in the number of requests to intelligence authorities to strengthen international security. These requirements open a new opportunity for increased security and intelligence cooperation between the special services of the participating countries, as well as those interested in participating in this process. The serious threat posed by international terrorism and the danger of internal revival are the basis for the widest possible cooperation between different countries. The concept of security from the perspective of international organizations, governments and the public has expanded significantly in many areas since the end of the Cold War. The focus of

special services is now centred not only on the security of their own countries, but also on the security of other states.

However, the growing demands for the involvement of the intelligence sector in the work of ensuring international security go beyond the objectives of conflict prevention, crisis management, and the provision of information on peacekeeping operations. Intelligence agencies activities address another group of global long-term security issues. The processes of preventing and combating terrorism, in which the intelligence authorities play the most important role, are an example of such problems. Another example is the problem of limiting weapons of mass destruction and the proliferation of conventional weapons. International sanctions are the next category, according to which the special services are assigned the role of intelligence and analytical support of the activity of law enforcement authorities in combating drug trafficking, money laundering and other forms of organized crime. Last but not least, there is a dynamic need for international cooperation in protecting both national critical infrastructures, characterized by vulnerability to terrorist attacks, and global communications networks.

Conclusion

Secret actions, a less common task for foreign special services, are increasingly being discussed as a necessary part of the work of the intelligence authorities of contemporary democratic states. There is also a relative mismatch between global cooperation and traditional monitoring and counterintelligence mechanisms, which have always been national in nature. On the one hand, the need for cooperation, coercion and mutual support has been imposed as an imperative and as a vital need to ensure the responsiveness of intelligence authorities to contemporary threats, and on the other hand, the same security threats and risks require reconsideration.

The importance of the defensive side of intelligence activity, contrary to the fact that the prospect of a potential "traditional" conflict may seem incredible, remains open to research. Intelligence agencies must be able to guarantee the protection of the authenticity of sources of information and their confidentiality, and the conditions for

cooperation must completely exclude the vulnerability of such guarantees. Expecting this imperative is important not only for the information authority itself and its staff, but also for the people, who in one form or another cooperate with these authorities. The need for secrecy is due to the fact that it is the only way to ensure the security of existing and potential sources of information.

References:

1. Igor Munteanu. (2010). *Political review and parties' recommendations legislation for reform in Moldova*. IDIS "Viitorul".

2. *Concepţia securităţii naţionale a Republicii Moldova,* adoptată prin Legea nr. 112- XVI/22.05.2008. *Publicat în Monitorul Oficial,* nr. 97-98/357 din 03.06.2008.

3. *Strategia securităţii naţionale a Republicii Moldova*, adoptată prin Hotărârea Parlamentului, nr. 153/15.07.2011. *Publicat în Monitorul Oficial,* nr. 170-175/499 din 14.10.2011.

4. Law no. 1/ 1998. (Lege nr. 1 din 6 ianuarie 1998 privind organizarea şi funcţionarea Serviciului de Informaţii Externe). *Publicată în Monitorul Oficial,* nr. 511 din 18.10.2000.

5. Sun Tzu. (2000). *Arta războiului*. Bucureşti: Cartex.

6. C. Troncotă, H. Blidaru. (2010). *Constituirea Comunităţii europene de informaţii – o posibilă soluţie la provocările începutului de mileniu în planul securităţii*.

ACTIVE MEASURES COUNTERINTELLIGENCE RECONFIGURATION ELEMENTS

Florin BUŞTIUC[*]
Mircea STAN[*]

Abstract:
In general, counterintelligence is a process of detecting, preventing, exploiting and manipulating the intelligence activities of opposing/external entities (groups, organizations, states), and is usually explained as protection of secrets against espionage (counterintelligence). In particular, in some states, in addition to the classic intelligence activities, clandestine/covert operations (in Western terminology) or active measures (in Soviet/Russian terminology) are conducted. By means of such operations the decisions or events, the political, military or social circumstances in another state are influenced in order to promote own foreign policy objectives. Such operations are conducted by intelligence structures, as they have available specialized personnel and specific skills, necessary for the complex integration of various resources and techniques to exercise influence. Taking this aspect into account, it should come as no surprise that the approaches used in order to identify and neutralize such operations get materialized in the area of counterintelligence. The paper is aimed at exploring some active measures which could be used to reconfigure counterintelligence, becoming then relevant for an effective national security policy. A comparative analysis between the two former Cold War superpowers – the USSR and the US – is performed in order to exemplify and support the arguments presented while also underlining the peculiarity of Soviet (present day Russian) conducts. In the first instance, the historical perspective/lens is used to account for the patterns developed during the Cold War, and then, shifting to the current status-quo, their relevance is explained in the present-day context.

Keywords: *intelligence, counterintelligence, espionage, counterespionage, active measures.*

[*] PhD, "Mihai Viteazul" National Intelligence Academy, email: florinnn11@yahoo.com
[*] PhD, "Mihai Viteazul" National Intelligence Academy, email: stanmircea90@gmail.com

Introduction

The fear of invaders present in the Russian mentality has resulted in generating the feeling of insecurity and inferiority to the "outside world", which has influenced their behaviour throughout history. Successive generations have had to adapt to the vicissitudes of time, using all possible means to protect and resist. The gap between the Russians and the other peoples, more advanced in terms of social, political, economic, military or cultural aspects, has been bridged through the "loans" the Russians have got to resist. Such "loans" have materialized, at the level of security and intelligence services, in active measures, a natural evolutionary process, based on fear and inferiority.

The activity of security and intelligence services is not limited to the field of intelligence/counterintelligence. Each state seeks to gain benefits by conducting clandestine/covert actions (Tucker, 2014, p. 73)[1]. The case of the Soviets is distinct because they have employed active measures. Due to opening several archives, today we know that other states have also used such methods, but the Soviets have perfected and transformed them into the foundation of their intelligence activity.

All the elements included in the active measures program (persuasion, influence, manipulation, disinformation, propaganda, subversion, – intoxication, deception, *maskirovka*[2] – rumours, reflexive control, fakes, sabotage, provocation, penetration, fabrication, compromise, conspiracy, combination) are considered (by the democratic world) morally reprehensible. To this extent, they are further perceived as diachronic, time-consuming, long-lasting, psycho-social processes and also as elastic, unpredictable concepts which cannot be studied according to a certain pattern. All are intended for permeable targets which include a set of peculiar characteristics: inconsistency, a certain degree of flexibility that allows them to adapt to

[1] Both types of actions are secret. The difference is that in the case of clandestine actions the act as such and those who perform it (agents – A.N.) are not known, while in the case of covert actions the entity that orders them (state – A.N.) is not known.

[2] In general the meaning is the same, the differences pertaining to semantics. In Romanian, the terms correspond to: *l'intoxication* (French), *deception* (English), *maskirovka* (Russian).

changing trends in the context. The origin of such active measures is also unusual as they emerge from certain vulnerabilities, low legitimacy or even illegitimacy while they seek to identify the primary impulses that influence the human psyche by penetrating its intimacy. The excessive employment of an active measures program can result in the initiator losing credibility; they create a linear process that generates certain situations that determine an attitude that, in turn, produces certain behaviour.

Consequently, there are no unanimously accepted definition, which makes it difficult to establish a scientific framework to highlight their implementation mechanisms, action forms, methods of counteracting etc. The attempt to define them rather leads to eclectic panoply of definitions.

Conceptual Distinction between Active Measures and Clandestine/Covert Actions

Without claiming to conduct an exhaustive analysis and starting from one of the classical definitions of espionage "(...) clandestine collection of intelligence" (Bennet, 2002, p. 8), from the Soviet perspective, active measures are often identical to espionage. There are many definitions of active measures that come to support the mentioned idea, one of them being provided in *Spy Book. The Encyclopaedia of Espionage*: "Russian term for intelligence operations that will affect another nation's policies or actions. These can be either covert or open and can entail a wide variety of activities, including assassination." (Polmar, Allen, and Thomas, 2004, p. 5)

Considering their cultural and operational specifics, the activities related to "clandestine collection of intelligence" (espionage-A.N.) conducted by the Russian specialized structures are subsumed under active measures, thus being outlined the idea of an "ideological/political warfare, having an extremely clandestine aspect" *grafted onto the* "*predestination*" for the employment of active measures. A possible explanation is that the "predestination" stems from the feelings of insecurity of the Russian Federation in relation to the West, such circumstances determining the perfection and

transformation of active measures into the foundation of Russian intelligence activity.

Considering the context in which the Russian Federation perceives the West (defined not geographically, but politically and culturally-A.N.) as a real threat, the intelligence services function in the paradigm of an existing war, applying the following principles: any decrease in the power status of the West/ any sign of instability becomes an implicit advantage for the Russian Federation; not only intelligence is collected but also active measures are usually employed; it is more appropriate for some events to be approached and exploited as opportunities than abandoned as possible failures (in comparison, in peacetime, Western institutions have a risk aversion due to potentially negative political or other effects). An integrated correlation of these principles explains the fast pace and current visibility of Russian active measures, reflected in aggressive actions in self-declared areas of influence (former Soviet states-A.N.) and visible in the West (interference in elections and disinformation-A.N.). (Galeotti, May 2017)

From a Western perspective (mostly American-A.N.), an equivalent concept for active measures is that of clandestine/covert operations, an aspect that also results from Soviet terminology, namely that the term "active operations *(aktivnyye operatsii)* is synonymous with «active measures», but indicates operations on a somewhat larger scale." (Mitrokhin, 2004, p. 13) Clandestine/covert actions represent that type of operational actions conducted to influence the course of international events or decision-makers, be they persons or organizations.

Covert actions are defined by Abram N. Shulsky and Gary J. Schmitt as follows:

> "In the US intelligence lexicon, refers to the attempt by one government to pursue its foreign policy objectives by conducting some secret activity to influence the behaviour of a foreign government or political, military, economic, or societal events and circumstances in a foreign country. As the term implies, the defining characteristic of covert actions is that government conducting the activity conduct it in a secret or covert manner.

> However, what secrecy means precisely can vary according to the particular circumstances." (Shulsky and Schmitt, 2002, p. 75)

In fact, covert operations are introduced in the US legislation, resulting that they are different in terms of content and means of action from the intelligence/counterintelligence activity – their purpose is not to obtain information, but to promote certain national interests abroad:

> "(...) the term «covert action» means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:
> (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of the United States Government programs, or administrative activities (...)." (*Intelligence Authorization Act*, 1991, p. 443-444)

Given that each state attempts, depending on its resources, to create advantages by conducting clandestine/covert actions, it results that the activity of special services is not limited to the field of intelligence/counterintelligence. In this regard, some authors, such as Eric Rosenbach and Aki J. Peritz, appreciate that the activities of the services are reflected in: a) collection, analysis and production of relevant information to support the decisions of political factors in the field of security, defence and public order – information activity; b) protection of activities and results through counterintelligence activity; c) execution of clandestine/covert operations. (Rosenbach and Peritz, 2009, p. 10) Arthur S. Hulnick argues that the involvement of such structures in conducting clandestine/covert operations is justified as they have the necessary capabilities and specialized personnel. (Hulnick, 2006, p. 976) However, in the USA, there are also theoretical approaches that question this aspect, according to Shulsky and Schmitt (2002, p. 95-97).

Clandestine/covert actions as well as active measures can be treated as instruments of foreign policy or components of security and

intelligence services. The major difference between clandestine/covert actions and active measures is given by the leadership models: a totalitarian regime will easily employ human and material resources in conducting active measures, without considering legal or ethical aspects, while in democratic regimes the law is obeyed and security and intelligence services are under strict control. For example, the Communist Party of the Soviet Union (CPSU) concentrated all the state power and had no difficulty in giving directives for the implementation of the active measures program. On the other hand, democratic governments, especially the US one, would have encountered obstacles in centralizing the necessary decisions for the implementation of some clandestine/covert actions. (Godson and Shultz, 1985, p. 101-110)

Another difference in terms of doctrine refers to the fact that while in the USA the foundation of the intelligence services activity is the collection and capitalization on the data from covert sources (Shulsky and Schmitt, 2002, p. 126), in the USSR active measures used to be the foundation of the services activity, entailing both covert and public/overt modes of action, "(...) certain overt and covert techniques for influencing events and behaviour in, and the actions of, foreign countries". (Shultz and Godson, 1984, p. 193) Clandestine/covert actions are instruments that support the US foreign policy, namely an aggregate of military actions and diplomacy (the CIA is the government institution legally authorized to conduct such actions, the goal being to make impossible the identification of the initiator). (Daugherty, 2010, p. 623 and 2004, p. 25; Macgaffin, 2005, p. 83; Bennet, 2002, p. 54)

In the USSR, the KGB-GRU conducted clandestine/covert actions outside the country, which were aimed at three general areas: political, economic, and scientific. Where technology theft was unsuccessful, sabotage was practiced to delay as much as possible the achievement of a patent for a product or invention before it appeared in the USSR. The Kremlin also capitalized on the agitation potential of left-wing movements, where they existed and could overthrow the constitutional order.

The USSR was unequalled in terms of the diversity and refinement of its covert efforts to undermine the credibility of the US government domestically, to discredit it, to disrupt its foreign policy, to

generate and amplify the dissent between allies, thus transcending the traditional limits of diplomacy and of diplomatic and intelligence activities. The panoply of activities – based on KGB-related operations and connected to the party foreign policy departments – includes media manipulation, influencers, associations and groups of protestants/ influencers/activists, propaganda and disinformation, subsumed under the name of "active measures", a major instrument of Soviet foreign policy. In this context, counterintelligence plays a significant part in countering this type of threats. However, it is not the only one involved as the actions meant to raise the awareness of the officials, of the mass media, of the domestic public, public diplomacy, covert activities and counterintelligence (by identifying and neutralizing the activities and the internally involved people – A.N.) provide an effective multiple response. (CIA document, May 1, 1986, p. 1-7)

The Connection between Active Measures and *Counterintelligence*

Richard A. Posner (2009, p. 261) sees counterintelligence in a classical way, as representing the efforts to prevent any covert activity directed against national security, from counterespionage to the identification of the dormant networks that could be activated for acts of sabotage or terrorist attacks.

A. C. Wasemiller introduces an extensive approach to counterintelligence, translated into "protecting a legally established government against covert attacks/clandestine activities", as the state has different protection mechanisms and structures in case of overt aggression. The label of clandestine refers to the fact that the opponent tries to hide own activities such as espionage, subversion, sabotage or to camouflage its involvement as a "sponsor" of some covert actions. Consequently, the counterintelligence responsibility is to identify and transmit to decision-makers comprehensive information about foreign entities, the essential condition being for the data to be collected and transmitted in a secret manner, namely protected. (Wasemiller, 1994) In this context, intelligence and counterintelligence activities generate an intelligence product that is "almost a by-product of a governance

concept that often entails and relies on a secret support infrastructure". (Davies and Gustafson, 2013, p. 291)

A current imperative in terms of counterintelligence is to overcome the classical limitation to the protection of government secrets and corporate intellectual property (by neutralizing the recruitment of targets) and to focus on the efforts meant to divide the society and make it vulnerable. Soviet active measures were aimed at dividing the society and undermining the citizens' trust in their own institutions, as relevance being subsumed under the classical process of recruiting and exploiting secret human sources. Currently, they have been supplemented with an ingredient such as social networks, amid the "online tribalism" the possibility of expanding the fissures of society by disseminating fake news being amplified. (Costa and Geltzer, 2019)

The active measures employed by the USSR were mainly intended against the USA and, under those circumstances; they stimulated the development of American counterintelligence. (Sudoplatov et. al., 1994, p. 5; McNamara, 2010, p. 2) Thus, in order to monitor active measures, in 1981, it was established in the USA an interagency cooperation structure – Active Measures Working Group – which consisted of representatives of the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Department of Defence (DoD), the Arms Control and Disarmament Agency, the Defence Intelligence Agency (DIA), the Department of Justice and the United States Information Agency. The mentioned structure (disbanded following the dissolution of the USSR-A.N.) made public different materials, namely: "Forgery, disinformation and influence operations of the USSR in US documents (1981)," "Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns (1986)," "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987 (1987)," 'Disinformation, The Media, and Foreign Policy (1987)," "Soviet Active Measures in the Era of Glasnost (1988)," "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987 (1989)," "Soviet Active Measures in the 'Post-Cold War' Era 1988-1991 (1992)."

The study of active measures is a topical theme. For example, the "Institute of World Politics' publishes the academic journal "Active

Measures" (https://www.iwp.edu/category/active-measures/); the "Centre for Eastern Studies" in Poland published, in 2017, "Active measures. Russia's Key Export" (2017); under the aegis of the "European Centre of Excellence for Countering Hybrid Threats/Hybrid COE Strategic Analysis," in 2018, it appeared the study "The resurrection of «active measures»: Intelligence services as a part of Russia's influencing toolbox." (https://www.hybridcoe.fi/)

Foreign/External Influence Operations – Means of Action of Current Active Measures

Relating to active measures, from the perspective of counterintelligence, the term foreign/ external influence is used, which is why we appreciate that it is an approach that correctly reflects an effect-means relationship: influence is a result of various activities/means employed by adverse foreign entities, regardless of the degree of topicality and upgrade, using social and technological elements. In fact, traditionally, in addition to the collection of open source information (and the use of technology to collect secret information – A.N.), security and intelligence services conduct recruitment activities (subsumed under "classical espionage") to access information of interest – the aim is to obtain information on political decision-making and sometimes to influence decision-making processes. (https://www.supo.fi/vastatiedustelu)

Influence operations – including covert actions conducted by foreign governments to influence the public or political arena – are not new, but the interconnection of modern society coupled with the resources of the Internet has amplified the impact of this threat. (https://www.fbi.gov/investigate/counterintelligence/foreign-influence)
Foreign influence, positioned as influencing a state's domestic policy (and possibly associated with information warfare), is a threat to the constitutional order and it can be achieved directly by various foreign state entities, including security and intelligence services or indirectly by using "compatriots/ethnic groups" as a political pretext. In this regard, the normal interest of a foreign state in providing linguistic and cultural support differs visibly from the objective of influencing the decision-making process of another state through financial

interventions and the rhetoric of official and unofficial declarations. (https://www.kapo.ee/en/content/influence-activities.html)

Counterintelligence identifies the activities initiated by foreign authorities and by natural or legal persons (mainly intelligence services) acting in the interests of foreign authorities. From this perspective, counterintelligence has the following major functions: a) informative – information is collected, records are made and information about the activities, interests and intentions of foreign authorities is sent to legal beneficiaries; b) preventive – measures are recommended or adopted to prevent or disrupt foreign intelligence activities. The preventive function is aimed at: avoiding the leakage of classified information; obstructing openly or discreetly the activities of foreign intelligence services; detecting and disrupting the operations through which the influence of foreign authorities is achieved and extended through disinformation, manipulation, deception, propaganda etc. (https://www.bis.cz/counterintelligence/)

From the FBI's perspective, foreign influence operations refer to: the classical targeting of officials and other persons through the classical methods of intelligence activities; the use of fake identities and narrative elements fabricated on social platforms to discredit individuals and institutions (there is an increased diffusion of disinformation, contradictions/tensions are generated to undermine trust); illegal actions affecting the voting process and financing the campaigns; cyber-attacks on voting infrastructure, along with computer-type intrusions targeting elected officials and other people. (https://www.fbi.gov/investigate/counterintelligence/foreign-influence)
In 2017, within the FBI it was established the "Foreign Influence Task Force (FITF)", which is aimed at identifying and countering the foreign influence operations targeting democratic institutions.

The FBI has also developed the "Protected Voices project", which provides tools and resources (including from the Department of Homeland Security and the Director of National Intelligence) for protection against online influence operations. Threats include cyber-attacks on political campaigns and government infrastructure (hacking and extracting sensitive information from computers, databases, networks, telephones and e-mails); secret funding or influence

operations to support or denigrate a person or cause (political publicity by foreign groups declaring themselves US citizens, illegal campaign contributions); disinformation on social media platforms (e.g., intentionally disseminating fake or incoherent information about a social issue to provoke all parties and stimulate conflict, see: https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices).

Related to foreign influence, it is necessary to present counterintelligence functions[3]: a) collection of data regarding foreign intelligence entities and their activities using open or clandestine sources; b) study and analysis of their structure, personnel, activities and operations; c) operations meant to disturb and neutralize the adversaries activities (Moravej and Díaz, 2007), and Jeffrey Richelson (2016, p. 544) adds d) investigation of involved people, and e) support for operations. Michelle K. Van Cleave (2013, p. 60-64) invokes some specific sequences – identification, assessment, neutralization and exploitation of the adversary activities (neutralization also includes the categories established by Arthur S. Hulnick (2006, p. 14) as well as informative penetration and success publicity-A.N.).

Conclusions

Counterintelligence should consider covert activities (usually to promote subversion) a significant threat, derived from the Cold War period. It is more important in the context in which adverse entities, regardless of ideology, use the same underground tactics in their invisible attempt to influence and force "gaining loyalty" to a democratic society. Given that the central bureaucratic systems are inadequate in relation to the threats posed by "agile transnational networks" the effective protection is achieved through education at national level as the "best defence of a nation is an informed citizen".

One of the ways to detect/identify subversive activities (aimed at discrediting and undermining the power, regime or a social situation in a given territory – A.N.) – and by extension active measures/

[3] One of the functions is "defectors assessment", but we consider it is not independent, being included in the area of foreign services study and analysis.

influence operations – is awareness, through which citizens are cognizant of the threats posed by subversive activities and assimilate the ways to recognize them, while the competent structures communicate the contact details for the reported cases. Logically, if the inquiries/investigations and assessments of threats are conducted by experts, the specific means of detection/identification – surveillance and cooperation between state or private structures – are supplemented with awareness, where the citizen becomes an active part. Related to the idea of awareness, in an asymmetrical threat environment, the effectiveness of counterintelligence derives not only from external partnerships but also from internal practices.

References:

1. Bennet, Richard M., (2002). *Espionage. An Encyclopaedia of Spies and Secrets*, London, Virgin Books.

2. CIA. (May 1, 1986). *Thwart Activities of Foreign Powers which Constitute Interference in US*, declassified.

3. Costa, Christopher P., Geltzer, Joshua A. (October 14, 2019). "To Fight Disinformation, Rethink Counterintelligence", *Defence One*.

4. Daugherty, William J. (2004). *Executive Secrets: Covert Action and the Presidency*, USA: University of Kentucky Press.

5. Daugherty, William J., (2010). "Covert Action: Strengths and Weaknesses" in Loch K. Johnson (ed.), *The Oxford of National Security Intelligence,* New York: Oxford University Press.

6. Galeotti, Mark. (May 2017). "Russian Intelligence Is at (Political) War", *NATO Review*.

7. Godson, Roy, Shultz, Richard. (1985). "Soviet Active Measures: Distinctions and Definitions", *Defence Analysis,* Vol. 1, No. 2.

8. Hulnick, Arthur S. (2006). "What's wrong with the Intelligence Cycle", *Intelligence and National Security*, vol. 21, issue 6.

9. Kaveh Moravej, Gustavo Díaz. (January 2007). "Critical Issues in Contemporary Counter-intelligence", *UNISCI Journal*.

10. McNamara, Francis J. (2010). *U.S. Counterintelligence Today,* Washington DC, The Nathan Hale Institute.

11. Mitrokhin, Vasili. (2004). *KGB Lexicon: The Soviet Intelligence Officers Handbook*, London: Routledge.

12. Macgaffin, John. (2005). "Clandestine Humint Intelligence. Spies, Counterspies and Covert Actions", in Jennifer E. Sims, Burton Gerber (ed.), *Transforming U.S. Intelligence*, Washington DC: Georgetown University Press.

13. Philip H. J. Davies and Kristian C. Gustafson (eds.) (2013). *Intelligence Elsewhere: Spies and Espionage outside the Anglo sphere*, Washington DC: Georgetown University Press.

14. Public Law 102-88-102d Congress, *Intelligence Authorization Act*, Fiscal Year 1991, Aug. 14, 1991, [50 USC 413b].

15. Polmar, Norman, Allen, B., Thomas, B. (2004). *Spy Book. The Encyclopaedia of Espionage*, New York: Random House Reference.

16. Posner, Richard A. (2009). "Counterintelligence, Counterterrorism, Civil Liberties, and the Domestic Intelligence Controversy" in Jennifer E. Sims and Burton Gerber (eds.), *Vaults, Mirrors, and Masks: Rediscovering US Counterintelligence,* Washington DC: Georgetown University Press.

17. Richelson, Jeffrey T. (2016). *The U.S. Intelligence Community,* 7th edition, USA: Westview Press.

18. Rosenbach, Eric Peritz, Aki J. (2009). *Confrontation or Collaboration? Congress and the Intelligence Community*, USA: John F. Kennedy School of Government, Harvard University.

19. Schoen, Fletcher, Lamb, Christopher J. (June 2012). *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Washington DC, Institute for National Strategic Studies.

20. Shulsky, Abram N., Schmitt, Gary J. (2002). *Silent Warfare: Understanding the World of Intelligence,* 3rd edition, Washington DC: Potomac Books Inc.

21. Shultz, Richard H., Godson, Roy. (1984). *Dezinformtsia: Active Measures in Soviet Strategy*, USA: Pergamon-Brassey's, McLean.

22. Sudoplatov, Pavel, et.al. (1994). *Misiuni speciale: arhitectura terorii*, translated by Anca Irina Ionescu, Ploiești: Editura Elit Comentator, Editura Eleusis.

23. Tucker, David. (2014). *The End of Intelligence: Espionage and State Power in the Information Age*, California: California, Stanford University Press.

24. Van Cleave, Michelle K. (2013). "What is Counterintelligence? A Guide to Thinking and Teaching about CI. From AFIO's", *Journal of U.S. Intelligence Studies*, Vol. 20, No 2.

25. Wasemiller, C. A. (1994). *The Anatomy of Counterintelligence* (SUA: CIA, Center for the Study of Intelligence, Vol. 13, No. 1.

26. https://www.iwp.edu/category/active-measures/

27. https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export
28. https://www.hybridcoe.fi/
29. https://www.supo.fi/vastatiedustelu
30. https://www.fbi.gov/investigate/counterintelligence/foreign-influence
31. https://www.kapo.ee/en/content/influence-activities.html.
32. https://www.bis.cz/counterintelligence/
33. https://www.fbi.gov/investigate/counterintelligence/foreign-influence
34. https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY

NEW GEOPOLITICS, NEW ARGUMENTS. CAN THE EU KEEP UP THE PEACE IN THE GLOBAL SECURITY SYSTEM?

Iuliana UDROIU*

Abstract:
The COVID-19 pandemic, rough relationships between the most important geopolitical actors (the USA and China), the constant shifts of terrorist phenomenon, and the zombification of economy - all of these are early signals that the global security system is in great distress. The UN seems to lose the compass in this dynamics, failing to provide informed and strong answers to the crisis, giving up control to smaller, regional or specialised, and more practical institutions. In this context, it seems that the EU gets a new opportunity to shape the global security environment, as it has all the instruments necessary to tackle it.

Keywords: *EU, strategic autonomy, crisis management, multilateralism*.

The frame of reference of the EU's position in the global security system

In a security environment where geostrategic competition has gained unpredictable values, the EU is, despite some punctual slippages driven by personal ambitions of the leaders of the Member States, a pole of stability. The spectrum of a legitimacy crisis remains current after Brexit, but for medium term the danger of an implosion is not quite possible. However, internal vulnerabilities and acting external threats put pressure on the future of a strategic EU.

Internally, the effects of the COVID-19 pandemic have brought some dose of uncertainty regarding the mobilization capacity of EU states, but the input of solidarity, despite occasional divergences on

* PhD, "Mihai Viteazul" National Intelligence Academy, email: iulia.udroiu@gmail.com

the allocation of resources, still proves once again, the ability to collectively manage internal security crises. States like Hungary and Poland will continue to be hotspots in European unity, even if for different reasons. Brexit is both a setback and a new opportunity to strengthen continental Europe.

Maintaining EU stability is not an easy task, given a transfer of difficult power in the US, its main global ally, which revealed multiple fractures from a social, horizontal, vertical and transversal point of view of this state. Historically speaking, the democratic rulings have always generated conceptual resettlements of directions of action in the US foreign policy towards the European space and global re-employment, including in geographical areas which have been moved to a secondary place by the Republican Administrations, such as the EU, Latin America and Africa, the latter also in the direct attention of the EU, China and India, alike. But good relations with the EU have always been a key element for the USA, being foreseeable a launch again of the transatlantic partnership, including on the security component. NATO will thus remain an instrument of transatlantic cooperation in which the eastern flank will become essential, including through an increased military presence. In their turn, China and the Russian Federation will court the EU as a strategic economically and a field for practicing soft strategies.

The competition between the US, China and Russia continues to set the international political agenda, on multiple security dimensions, such as the economic, cyber, or the social one. China's aggressiveness in asserting its own influence, on the aforementioned coordinates, lead to a political and security dependency of the EU, with which neither the US nor the Russian Federation will be satisfied. Accelerating the rivalry between the great global powers involves the need for greater cohesion between the EU member states, by defining a strategic common culture.

China is consistently strengthening its profile as a strong international player, capitalizing on the context created by the COVID-19 pandemic in order to be perceived as a generous protector supporting the countries in need, including EU member states, and trying to turn the health crisis into an opportunity to strengthen its ambitions of a global player with hegemonic desires. Beijing's attitude

and the race to take advantage of the opportunities generated by the COVID-19 pandemic in the health, information and economic sectors did not serve those who promoted the renunciation of protectionism.

In the long-term, China may seek to counterbalance US influence in the region, to consolidate the presence of Chinese companies, to influence changes in the EU's perspective compared towards the relevant files for Beijing and the validation of global power position.

In turn, the Russian Federation has shown an increasing level of aggression. Although unlikely to become a direct threat to the EU, in the absence of a trigger outside the European Union, the methods used, from 2008 onwards, to promote it regionally and internationally require a strategic attention from authorities in Brussels.

Aggressive new geopolitical actors in the immediate vicinity, such as Turkey, with hegemonic ambitions, add to the insecurity around the EU, using a tool of pressure and even blackmailing with the issue of illegal migration, in connection with that of terrorism.

Developments in other areas, such as Africa, Asia and South America, will also shape the EU's strategic position. As providers of terrorism and a source of illegal migration, the first two are in the direct attention of crisis mitigation programs and security actions. At the same time, all three geopolitical areas present opportunities for assertion of soft power of the EU; states such as India, Brazil, Saudi Arabia, and South Africa can be seen as strategic allies in imposing a global power system based on multilateralism.

Strategic autonomy – how to transform a crisis into an opportunity

In order to meet the new security challenges, both internal and external ones, the EU needs to consolidate its strategic autonomy.

The concept of autonomy or strategic sovereignty, often suspected to mask the hegemonic ambitions of France in the political strategic sphere, especially that of President Emmanuel Macron, is not a new one, being circulated in scholastic circles since the 1990s (*Livre blanc sur la Defence*, 1994, p. 49, 50, 52, and 139), but has gained new strength with the rise of global security challenges. Brexit and COVID-19 have, in particular, boosted the identification of one coherent

framework for its implementation. Critics have insisted that strategic autonomy is a recipient of new forms of European protectionism, a proof that the EU re-enters the sphere of geopolitical blocks, respectively the portrait of a "Europe" alone on the road. (*Zandee et. al.*, *December* 2020)

The operationalization of the concept quickly gained the support of many high-ranking politicians, being also included in the European "government programs" of the states taking over rotating presidency (Portugal being the most recent of these, during the first semester of 2021). From Josep Borrell's point of view, strategic autonomy is represented by the protection the EU's ability to act in accordance with European interests and reduce dependencies and vulnerabilities. (*Remarks by* the High Representative/Vice-*President Josep Borrell*, January 2021).

According to Emmanuel Macron, "based on strategic autonomy, the EU must find the means to decide for itself and not to depend on others" during short term crisis management, such as pandemics or terrorist attacks, but also on long term, such as the effects of climate change or the disruptive technological transition. To this end, it is necessary to reinvent useful forms of cooperation – project coalitions and players, the modernization of European structures and the creation of a uniform field of action, respectively the reconsideration of the terms in which the cooperation is viewed. (*The Macron Doctrine,* November 16, 2020)

Charles Michel chose to define strategic autonomy through his objectives: stability, dissemination of European standards and promotion of community values. (Speech by President Charles Michel, September 28, 2020)

The reason for its promotion, however, is difficult to dispute: in a period of geopolitical tension and instability, the EU must be able to act much more independently, to protect and promote their interests and values globally (Csernatoni, November 6, 2020). The EU needs to develop defence and response mechanisms to new challenges such as the new Trump Administration type, another soft crisis of continental or global magnitude, a revival of terrorism, etc. It is essential to gain the

EU's capacity to act alone, if necessary, at least until the mobilization of the Union's natural allies.

Most perspectives on strategic autonomy place it first in the hard field of defence and security capabilities. However, the priority direction in the implementation of the concept is focused on the soft dimension, respectively in civilian crisis management, with occasional military support (especially in the field of physical assurance). Its extensions go towards areas such as economics, finance and trade, regarded as intangible strategic assets.

Arguing, for example, the importance of outer space in ensuring autonomy, Josep Borrell mentions that space security requires improvement of situational awareness to manage security issues such as the response to disasters, surveillance of maritime and land borders and terrorist attacks. The centre satellite from Terrejon de Ardoz, the GALILEO, COPERNICUS or EGNOS programs are part of the tools used in this regard, the first proving useful even in the framework EU military operation IRINI in the Mediterranean. Referring to space security, the European official has moved into the hard dimension, appreciating that it involves the EUs ability to react in the event of a threat to European space assets and monitoring space traffic, this pillar allowing the use of space as a facilitator for European policies including the economic one. (*Remarks by* the High Representative/Vice-*President Josep Borrell*, January 2021)

In order to be put into practice, it is necessary to consolidate the EU's economic instruments and diplomacy and a plan of action to increase coherence in the relevant sectors to the external dimension, to strengthen resilience and the capacity to act, to reduce vulnerabilities and dependencies of Member States in areas such as economy, digital, energy, connectivity etc.

This implies internal consolidation, with Germany and France as a hard core, in order to be able to project soft power on the outside, without competing directly with the great powers, on the principle of resilience and by seizing opportunities, focusing at European level on priority issues and delegation to the Member States, through dedicated programs, of the mitigating task of the secondary threats. Cohesion and solidarity will govern the directions to strengthen the European project.

The coordination of efforts on the component of crisis management is expected, especially in the field of public health, and, in parallel, by focusing on the post-pandemic recovery of the European economy. But the order of priorities is rapidly changing, so flexibility is needed: recent examples of security crisis management are: 2008 – economic crisis; 2015 – illegal migration (influx of migrants from conflict areas, in line with organized crime and people trafficking, terrorism); 2020 – the COVID-19 pandemic, already burdened by coordination problems, has shown that mitigation solutions can be found, in the short and medium term, through focusing tools and resources on key elements.

In the long term, investments are to be made in the environment, research and development, digitalization technologies, which will create flexible crisis management mechanisms.

In concrete terms, the consolidation of the EU's strategic projection must manifest in two dimensions: in the immediate vicinity and globally. In what concerns the former, the recovery of Turkey and the Western Balkans is necessary from Russia and the stabilization of Ukraine, by including them in pragmatic cooperation formats, focused on problems to be solved. Detachment of Ankara from Moscow's policies is unlikely to succeed in the short run, as long as energy and political blackmail work – the case of Azerbaijan being the latest example.

Serbia's apparent strategic orientation towards the EU, by supporting the common position on the situation in Belarus, in the summer of 2020, was contradicted by the re-imposition of the Russian-Serbian strategic energy partnership by launching the Turkish Stream pipeline on the Serbian section, the renewal of Russian strategic acquisitions and the resumption of influence actions on the status of Kosovo. Moscow put its levers into operation concerning Montenegro, Bosnia and Herzegovina, by stimulating their institutional dysfunction.

With regard to Ukraine, the EU's aspirations can only be in the sense of its political and economic stabilization, the national antagonism being too strong in this state to implement any policies, in the short term.

At the global level, it is necessary to promote multilateralism, an open trade agenda and immediate help in crisis management/disaster

consequences (*Priorities 2019-2024*). Strategic autonomy is needed to avoid turning the EU into a "theatre of operations" between China, Russia and the USA. It is clear that US interests in Europe include the prevention of expanding Russia's geostrategic influence, using the energy factor and the actions of disappointment, with Hungary and the Balkan states as the spearhead, respectively China, which uses 5G commerce and technology as the "Trojan Horse".

Against this background, the antidote is to increase efforts so as to better connect economic policy with security interests, mainly by diminishing dependencies at industrial level, more closely filter foreign direct investment and to enhance synergies between the civilian and army industries. Other important elements target supplementing investments in defence, strengthening the EU's role as a global security guarantor, including in the field of maritime security, strengthening the European pillar within NATO and identifying solutions to improve cooperation and coordination between the EU and the Alliance.

The strengthening of EU military missions and operations through strengthening of European crisis management structures and more consistent efforts for revitalization of PESCO should not be overlooked, in a way that generates concrete results in the second stage of this initiative (2021 – 2025).

The results of massive investments and the achievement of strategic autonomy should also be a maturation of European defence, based on the future technology, to provide the EU with an umbrella in the face of unpredictable evolutions of the global security system. Complementary or not, NATO and the EU must cooperate, respecting the particularities of each institution.

EU strategic instruments

Hard crises are unlikely in the EU, but the number of soft crises will increase. Instruments of crisis management will thus have to be adapted to this trend, taking into account the political dimension and the economic/financial and operating dimension.

Politically, the Annual Foresight Report (October 2021), launched by the EC on September 9th 2020, sets out the challenges facing the EU in the medium and long term, putting the basis of

a methodology for strengthening resilience, promoting open strategic autonomy (European Commission press release of Maros Sefcovic, Vice-president of EC). Closely related to the concept of geopolitical resilience, open strategic autonomy is defined as the EU's commitment for open and fair trade, while preserving the benefits of the open economy and its global partners supporting it to lead a new and invigorated form of multilateralism which the world needs (COM(2020)45).

The open strategic autonomy model aims to define a new system of global economic governance and the development of mutually beneficial bilateral relations, protecting themselves, at the same time, from unfair and abusive practices. Thus, it will contribute to diversifying and strengthening of global supply chains to protect us from future crises and the strengthening of the international role of the European currency. (COM (2020)45)

In financial terms, the European Defence Fund, The Recovery and Resilience Facility and Next Generation EU, are, on a medium-term basis, a baseline for the management of immediate consequences of the crises and the recovery of the EU economy.

The European Defence Fund, launched in 2017, allocates funds worth of €205 million, aimed at increasing the strategic autonomy and industrial competitiveness of the EU (European Commission press release on European Defence Fund, June 15, 2020). On 15.06.2020, the Commission announced that the amount will finance 19 pan-European projects in the field of defence and disruptive technologies. It was announced as a financial instrument that will facilitate a good spending through a combined expenditure, by reducing fragmentation and inefficiency (Margarethe Vestager, Executive Vice-President of the Europe Ready Initiative for the Digital Age), respectively projects that strengthen resilience and strategic autonomy of the EU (Thierry Breton, Commissioner for the Internal Market). (European Commission press release on European Defence Fund, June 15, 2020)

Next Generation EU provides, for a limited period (2021-2024), for response and recovery measures in crisis situations, €500 billion in the form of grants and €250 billion in loans to Member States. Investments are grouped into 3 dimensions: investments and reforms meant to contribute to the solution of crises, launching again the EU by

stimulating private investment, and implementing lessons learned from crises. Areas such as health and preparation for future health crises are targeted, also research and digitalization, strategic investments and critical infrastructure. (Infografic Consiliul UE, 2020)

The Recovery and Resilience Facility, worth €672.5 billion, is channelled to investments in: competitiveness, productivity, environmental sustainability, education, health, employment and economic, social and territorial cohesion, green and digital transition. (Council of EU press release, December 18, 2020). To these a series of tools focused on "problems to be solved" (to-do list) are added.

The REACT-EU package will provide €47.5 billion additional support from current cohesion policy programs. The funding will be targeted at sectors that are of particular importance for an ecological, digital and resilient recovery. They have in view investments for the recovery of the labour market, short-term work schemes, youth employment measures, support for health systems and the provisions of capital work for small and medium enterprises. This support will be available to all economic sectors, including tourism and culture and for essential investments for ensuring the ecological and digital transition, consolidating some already planned investments in the framework of future cohesion programs. (*Cohesion policy action against coronavirus*, 2020)

EU4Health will have a budget of €9.4 billion to strengthen health security and preparedness for future crises in this field. (European Commission, 2021) InvestEU will be supplemented with €15.3 billion in order to mobilize private investments in projects across the Union. By the information dated June 19th 2020, the EU announced that the program will be expanded on a fifth dimension to take into account future needs of the European economy and to promote and secure the EU's strategic autonomy. (*InvestEU Programme*, 2021) An additional €16.5 billion will be provided for external actions, including humanitarian aid[1] to support Europe's global partners. The RescEU strategic reserve will receive an additional €2 billion from the Civil Protection mechanism of the EU for Subsidy and Procurement Managed

[1] Through *The Neighbourhood, Development and International Cooperation Instrument* (NDICI), also known as Global Europe, and The Humanitarian Aid Instrument.

by the Commission to increase the Unions's capacity to prepare for and respond to future crises. (*European Civil Protection and Humanitarian Aid Operations*)

Instrumentally, the EU has begun to strengthen its status and operational capacity of Community agencies, such as the European Centre for Disease Control, European Medicines Agency, European Defence Agency, and European Union Agency for Cybersecurity to be able to anticipate, manage and coordinate the response to crises.

A feasible actionable tool is represented by connectivity projects, as well as the Three Seas Initiative. Strongly supported by the USA, the Initiative was created in 2016 to facilitate the implementation of political, trade, energy and infrastructure projects in Southern, Eastern and Central Europe, in order to increase cohesion, convergence and security to the states in this area, as a premise for strengthening EU resilience and counterbalancing Russia's and China's influence.

Conclusion

Niche capabilities acquired through diplomatic exercise and crises management are now proving to be an important asset of global political assertion and act as a power factor in regions once difficult to penetrate. The basic condition, however, is for the European Union to go beyond its own systematic defects and identify solutions to increase cohesion and reduce disparities between the old and the new Europe, but also for the continuation of the enlargement process towards the Western and Eastern Balkans, where the best opportunities for soft power are found.

Achieving strategic autonomy by the EU can provide the frame of reference in order to achieve this desideratum; the main effect will be found, in essence, for the benefit of the security of European citizens. Strategic autonomy must, nevertheless, be seen not as a concept, but as a project, to which we attach objectives, a plan of action and a roadmap. It can also be considered an intermediate, important step in achieving guaranteed European sovereignty of a genuine European political force.

References:

1. COM (2020)45 final, *Europe's moment: repair and Prepare for the next Generation*. Available on https://eur-lex.europa.eu/legal-content/EN/TXT/?url=CELEX:52020DC0456, accessed on 21.01.2021.

2. Council of UE. (2020). *Infografic - Next Generation EU – pachetul de redresare în urma pandemiei de COVID-19*. Available on https://consilium.europa.eu/ro/infographics/ngeu-covid-19-recovery-pachage/, accessed on 26.01.2021.

3. Council of EU press release. (December 18, 2020). *Recovery and Resilience Facility: Council presidency and Parliament reach provisional agreement*. Available on https://www.consilium.europa.eu/ro/press/press-releases/2020/ 12/18/recovery-and-resilience-facility-council-presidency-and-parliament-reach-provisional-agreement/, accessed on 25.01.2021.

4. Csernatoni, Raluca. (2020). *EU Security and Defence Challenges: Toward a European Defence Winter?* Available on carnegieeurope.eu/2020/06/11/eu-security-and-defense-challenges-toward-european-defense-winter-pub-82032, accessed on 15.01.2021.

5. European Commission (2019), *Priorities 2019-2024.* Available on https://ec.europa.eu/info/strategy/priorities-2019-2024_ro

6. European Commission press release of Maros Sefcovic, Vice-president of EC (2021). Available on https://ec.europa.eu/commision/presscorner/detail/ro/ip_20_1586accessed on 15.01.2021.

7. European Commission annual foresight report. (October 2021). "New push for European Democracy". Available on https://ec.europe.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/strategic-foresight-report_en, accessed on 25.01.2021.

8. European Commission press release. (June 15, 2020). *European Defence Fund: €205 million to boost the EU's strategic autonomy and industrial competitiveness*, Brussels. Available on https://ec.europa.eu/commision/presscorner/detail/en/IP_20_1053, accessed on 15.01.2021.

9. European Commission. (2020). *Cohesion policy action against coronavirus*. Available on https://europa.eu/regional_policy*en*newsroom/coronavirus-response/react-eu, accessed on 25.01.2021.

10. European Commission. (2021). „UE pentru sănătate" 2021-2027 – O viziune pentru o Uniune Europeană mai sănătoasă. Available on https://ec.europa.eu/health/funding/eu4health_ro, accessed on 25.01.2021.

11. *European Civil Protection and Humanitarian Aid Operations.* Available on https://ec.europea.eu/echo/what/civil-protection/resceu_en, accessed on 25.01.2021.

12. InvestEU Programme. (2021). Available on https://europa.eu/investeu/home_ro, accessed on 25.01.2021.

13. *Livre Blanc sur la Defense*. (1994). Available on livreblancdefenseetsecurite.gouv.fr/pdf/le-livre-blanc-sur-la-defense-1994.pdf, accessed on 15.01.2021.

14. *Remarks by the High Representative/Vice-President Josep Borrell at the 13th European Space Conference*. (January 13, 2021). Available on Eeas.europa.eu/headquarters/headquarters-homepage/91401/space-remarks-high-representativevice-president-josep-borell-13th-european-space-conference_en, accessed on 16.01.2021.

15. *The Macron Doctrine. A Conversation with the French President*. (November 16, 2020). Available on https://geopolitique.eu/en/macron-grand-continent, accessed on 16.01.2021.

16. Speech by President Charles Michel to Bruegel think tank, (2020). "Strategic Autonomy for Europe – the Aim of Our generation". Available on https://consilium.europa.eu/en/press-releases/2020/09/28/l-autonomie-strategique-europenne-este-l-objectif-de-notre-generation-discours-du-president-charles-michel-au-groupe-de-reflexion-bruegel/, accessed on 25.01.2021.

17. Zandee, Dick, Deen, Bob, Kruijver, Kimberly, Stoetman, Adaja. (December 2020). *European Strategic Autonomy in security and defence*. Available on https://www.clingendael.org/publication/european-strategic-autonomy-security-and-defence, accessed on 25.01.2021.

FACTS FIRST: THE EUROPEAN APPROACH TO FAKE HISTORY. CASE STUDY – EU VS. DISINFO AND WWII MEMORIES

Mihaela TEODOR*
Bogdan TEODOR*

Abstract:
The European Union's concern about the use of propaganda, disinformation and fake history increased in the last period and the European Institutions has sought new strategies to counter these phenomena, including by fact-checking and fact promoting. Thus, the European approach suggests that fact-checking, debunking and deconstructing disinformation and fake history should constitute the core of countering all information influence activities. The simple premise of this "facts first approach" is that disinformation should be countered by ensuring that citizens have access to facts. In this paper, by using the special website of EU East Task Force, EU vs. Disinfo, we aim to build the map of the disinformation cases about WWII and Molotov-Ribbentrop Pact that circulated on the Russian or pro-Russian media between 2019 and 2021, and were deconstructed by the EU vs. Disinfo fact-checkers. By doing that we want to straight the role of euvsdisinfo.eu website in the fight against disinformation and fake history, and the importance of the European facts first approach.

Keywords: *Russian historical revisionism, fact-checking, fake history, EU vs. Disinfo, facts first approach.*

Introduction

The European Union's concerns about the use of disinformation and propaganda, especially by state actors, are increased. That is why the EU provided in the past seven years new strategies to combat and

* Senior Researcher PhD, "Mihai Viteazul" National Intelligence Academy, email: teodor.mihaela@animv.eu
* Associate Professor PhD, "Mihai Viteazul" National Intelligence Academy, email: teodor.bogdan@animv.eu

counter *fake news, fake history and disinformation*, including by fact-checking and fact promoting. This is called facts first approach, which simple premise is that disinformation should be countered by ensuring that citizens have access to facts. (MSB Report, July 2018) In the same way, countering fake history rely on the effort of historians to substantiate facts with *evidence*s (documents that prove with some certainty that events actually occurred.

In this research we used the definitions of the terms such as disinformation and fake news, which can be found in the literature and in official European Union documents. According to the report of the "European Commission's High-Level Expert Group on Fake News and Online Disinformation", the term "fake news" is considered "inadequate to describe the complex phenomenon of disinformation, which involves not necessarily fake, but fabricated content and practices going beyond the conventional news" ("A Multi-dimensional Approach to Disinformation", 30 March 2018). The European experts prefer the word "disinformation" instead and provide the following definition throughout the report: "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit". ("A Multi-dimensional Approach to Disinformation", 30 March 2018)

However, for the purpose of this paper, we will use the working definition of disinformation given by the European Commission in its official document "Tackling online disinformation: a European Approach" (April, 2018): "Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm."

Fake history is used in disinformation campaigns promoting false narratives about the European past, misinterpreting, twisting, or omitting important key facts in order to present victims as oppressors and oppressors as victims. This is the case of WWII memories, Europe being witness for the last three years to an unprecedented Russian historical revisionism. In this paper, by using the special website of EU East Task Force, EU vs. Disinfo, we aim to build the map of the disinformation cases about WWII and Molotov-Ribbentrop Pact that

circulated in the Russian or pro-Russian European media, between 2019 and 2021, which were deconstructed by the EU vs. Disinfo fact-checkers. By doing that, we want to straighten the role of euvsdisinfo.eu website in the fight against disinformation and fake history, and highlight the importance of the European *facts first approach.*

What EU has done so far to counter disinformation?

In 2015, the EU addressed *the Russian disinformation campaigns* and submitted the "Action plan on strategic communication", which was released on 22 June 2015. For the last seven years, based on this strategy, the European institutions called for measures to combat disinformation. As a result, the European Commission has taken more initiatives to protect citizens. Examples include the organization of a public consultation; the launch of a special Eurobarometer public opinion survey; the establishment of a High-Level Expert Group (HLEG); the publishing of a communication on "Tackling online disinformation: a European approach" (April 26, 2018); the organization of a multi-stakeholder conference (13-14 November 2018); the setting-up of a self-regulatory "Code of Practice" (September 2018 and official statement in 2019); the publishing of an "Action Plan to step up efforts to counter disinformation" in Europe and beyond (December 5, 2018), and a report on European Elections and Action Plan (2019); the redefining of the EU approach to countering hybrid threats (including propaganda and disinformation) in the new Security Union Strategy (2020); the publication of the "Joint Covid-19 Disinformation Communication" ("Tackling COVID-19 disinformation - Getting the facts right", June 2020); the establishing of the "European Democracy Action Plan: making EU democracies stronger" (December 2020). All these actions are represented in the following timeline:

Figure 1: EU key-actions timeline to counter disinformation (Authors' idea)

The results of the Eurobarometer, the "Report of the High-Level Expert Group", together with the results of the public consultation feed into the European strategy on how to tackle the disinformation presented on 26 April as "European Commission Communication. Tackling online disinformation: a European approach"(*April Communication*, 2018). It outlined the key principles and objectives in order "to raise public awareness about disinformation and tackle the phenomenon effectively, as well as the specific measures", including the "*support for an independent network of fact-checkers".* (*April Communication*, 2018)

Moreover, the *Action Plan* (December 2018) highlighted that fact-checkers were essential in tackling disinformation. In order "to strengthen fact checking, collective knowledge, and monitoring capacity on disinformation, the Commission committed, as a first step, *to support the creation of an independent European network of fact-checkers*" (*Action Plan*, December 2018). In this respect, in line with the *European Council conclusions* of March 2015, "a start-up team was established within the European External Actions Service (EEAS), with contributions from EU institutions and experts from EU Member

States". This team is known as "EU East StratCom Task Force" (ESTF), and reached full capacity by September 1, 2015 (See more on https://eeas.europa.eu). According to the official ESTF website, the new task force was focused on "proactive communication of EU policies and activities in the Eastern neighbourhood and beyond", and "better explaining EU policies in the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine)" (https://eeas.europa.eu). Moreover, the Task Force identified and helped journalists "to identify and compile what it believes to be false or fake news and to alert media outlets, Internet users, and the public of such disinformation" (https://euvsdisinfo.eu/). Two reports are published weekly: the "Disinformation Review" with the role to collect "examples of pro-Russian disinformation all around Europe and expose the breadth of the effort, including the countries and languages targeted"; and the "Disinformation Digest", which analyses how "Russian media sees the world and follows key trends on Russian social media." ("Questions and answers about the East StratCom Task Force", https://euvsdisinfo.eu/). The EU institutions and EU member states provide the unit members, which "report on and analyse disinformation trends, explains and exposes disinformation narratives, and raises awareness of disinformation coming from Russian State, Russian sources and spread in the Eastern neighbourhood media space." (See more on "Questions and answers about the East StratCom Task Force", https://euvsdisinfo.eu/)

The *Action Plan* (December 2018), re-endorsed ESTF's mandate from 2015 and recognised that ESTF has catalogued, analysed and put the spotlight on over "4,500 examples of disinformation by the Russian Federation". Now there are sixteen full-time staff having a diverse professional communications backgrounds and speaking several languages, including Russian ("The EU steps up action against disinformation", 5 December 2018). Moreover the *Action Plan* (December 2018) promoted "cooperation between European fact-checkers, and supported the creation of *an editorially European independent network*", by offering online tools to enable their collaboration. In 2018, there were 52 fact-checkers in Europe, but this number had not sufficient geographical coverage (Stencel and Griffin,

2018).[1] Moreover, the Commission deployed "a secure European online platform on disinformation, which offered cross-border data collection, analysis tools and access to EU-wide data, in support of cooperation between the fact-checking community and academics working on the problem of online disinformation." (*Action Plan,* December 2018)

The "Synopsis report of public consultation on fake news and online disinformation" (26 April 2018), states that "fact-checking through independent news organisations and civil society organisations is considered a method that better contributes to counter the spread of disinformation online." Thus, the European experts consider that presenting facts is a crucial technique for countering false information. However countering lies with facts can be problematic. It can be expensive, time-consuming, and may not reach the most vulnerable audiences. Furthermore, engaging with falsehoods can reinforce those stories through repetition; even if it should seek to create opportunities for reflection and debate as the activity of euvsdisinfo.eu website demonstrate.

Disinformation cases about WWII and Molotov-Ribbentrop Pact

According to the Kremlin's policy, the official Russian historiography is the only "true" way of interpreting the historical events about WWII. No documentary evidence is provided to support the affirmation and no dates are given to allow even the most superficial background check. Disinformation projects often defend the actions of the Russian Federation, directly or through selective agenda. Moreover, as Lucas and Pomerantsev (2016), state: "Kremlin propaganda also rebuts and deflects any criticism of Russia's own behaviour. All negative commentary about Russia is portrayed as either invented or unfair."

In this respect, we identified on the *Eu vs. Disinfo* website 65 disinformation cases about the WWII and Molotov-Ribbentrop Pact

[1] Some European countries as Hungary, Slovenia, the Netherlands, Malta, Luxembourg, Montenegro, Cyprus, Estonia, and Greece are not represented in the current state of play – nor have the capacity to keep abreast of the increasing volumes of online news content.

provided by the Russian or pro-Russian propaganda machine from 2019 to 2021 (See the Annex).

The following figure represents the distribution of the cases by year:

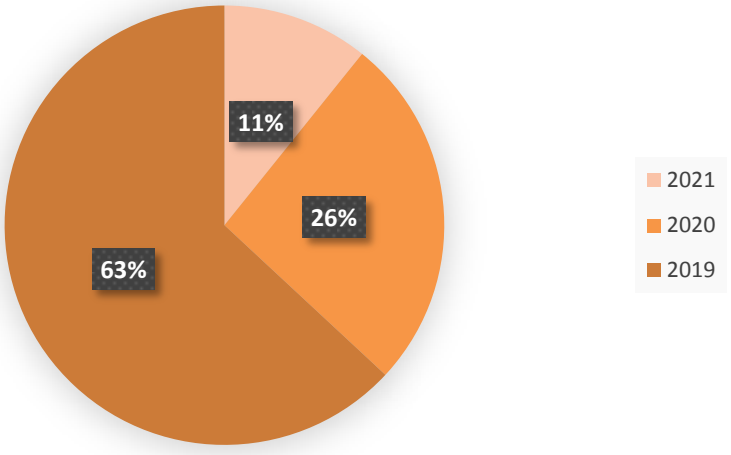


Figure 2: The distribution of disinformation cases about WWII and Molotov-Ribbentrop Pact by year (authors' idea)

Experts state that the Russian disinformation outlets are not the same in every country, the communication strategies usually being tailored specifically for the domestic audience, "embracing the digital age, exploiting the anonymity, ambiguity, ubiquity and flexibility of the Internet, in particular social media." (Lucas and Pomerantsev, 2016) It is the case of the Eastern Europe and Black Sea region countries facing the Russian disinformation activities, "disseminated both overtly – though foreign-language television (notably the multilingual RT) and the self-styled news agency Sputnik International – and covertly, using notionally independent journalists, experts and commentators as well as Internet trolls (paid propagandists)." (Lucas and Pomerantsev, 2016)

Moreover, disinformation and manipulation are spread abroad through their own official channels (i.e. RT or Sputnik), which are operational in several European languages, as we will see on the case

study proposed. From 65 cases, 34 were identified by Eu vs Disinfo staff on 12 different version of Sputnik, besides official Sputnik: Sputnik Mundo, Sputnik Deutsch, Sputnik Polska, Sputnik Serbia, Sputnik Estonia, Sputnik Armenia, Sputnik Lithuania and Lithuania Russian, Sputnik Italia, Sputnik Spanish, Sputnik Greece, Sputnik Georgia. Alternative outlets usually justify and legitimize the Kremlin's actions and narratives.

Analysing those 65 identified cases, we can state that Russian disinformation campaign and fake history narratives usually deal with a number of common topics, distributed by category in the following figure:

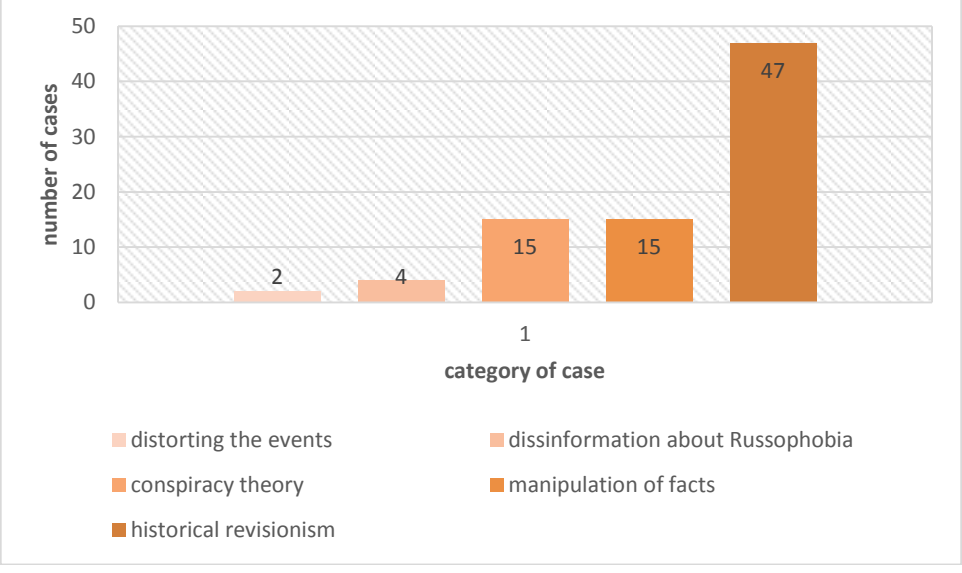


Figure 3: The distribution of disinformation cases about WWII and Molotov-Ribbentrop Pact by category
(Authors' idea based on categories identified on https://euvsdisinfo.eu/disinformation-cases/)

a. Promote the legitimacy of the policy for historical revisionism and deny the USSR's responsibility in the outbreak of WWII;
b. Manipulation of facts and propaganda narrative about the supposedly hostile anti-Russian intentions and policies of the aggressive West;

c. Pro-Kremlin conspiracy narrative about WWII and the Munich Agreement;
d. Disinformation narratives about Russophobia;
e. Distortion of the events which led up to the Second World War;

The starting point of the Russian fake history campaign was the 80th "anniversary"[2] from the day of the Molotov-Ribbentrop pact (23 August 1939) and Poland's decision not to invite the Russian delegation to WWII commemoration ceremony[3]. On that day, in contrast, Russian propaganda stressed that in 2019 is the *80th anniversary* of the Molotov-Ribbentrop pact. That is why, Estonia, Latvia, Lithuania, Poland, and Romania released a joint statement on the *80th commemoration* of the Molotov-Ribbentrop pact, urging "the governments of all European countries to provide both moral and material support to the ongoing historical investigation of the totalitarian regimes. By acting in a concerted manner, we can counter

[2] Commemoration vs anniversary: Ten years ago, the European Parliament proclaimed the 23rd of August as a European Day of Remembrance for Victims of Totalitarian Regimes. 23 August was chosen to coincide with the date of the signing of the Molotov–Ribbentrop Pact, a 1939 non-aggression pact between the USSR and Nazi Germany which contained a protocol dividing Romania, Poland, Lithuania, Latvia, Estonia, and Finland into designated German and Soviet spheres of influence. The European Day of Remembrance for Victims of Stalinism and Nazism, known as Black Ribbon Day in some countries, is an International Day of Remembrance for victims of totalitarian regimes, specifically Stalinism, Communism, Nazism and Fascism. It is observed on 23 August and symbolizes the rejection of "extremism, intolerance and oppression". It was designated by the European Parliament in 2008/2009 as "a Europe-wide Day of Remembrance for the victims of all totalitarian and authoritarian regimes, to be commemorated with dignity and impartiality", and has been observed annually by the bodies of the European Union since 2009. The purpose of the Day of Remembrance is to preserve the memory of the victims of mass deportations and exterminations, while promoting democratic values with the aim to reinforce peace and stability in Europe. See more on http://europeanmemories.net/events/european-day-of-remembrance-for-victims-of-stalinism-and-nazism/.

[3] In 2019, Poland decided not to invite the Russia to WWII commemoration ceremony, having to do with Russian aggression against Ukraine, being accused of promoting an "open policy of Russophobia". (https://euvsdisinfo.eu/disinformation-cases/)

more effectively disinformation campaigns and attempts to manipulate historical facts." (Joint Statement, 23 August 2019)

In 2019, Russia started the disinformation campaign using the distortion of the events which lead up to the Second World War and the historical revisionism to reinforce common pro-Kremlin disinformation narratives about WWII and the Molotov-Ribbentrop pact like:

"**The Molotov-Ribbentrop Pact played no role in unleashing World War II"** (see the annex) and **"USSR is not to blame for the beginning of World War II".** The Russian propaganda stressed that "the accusations against the Soviet Union and Josef Stalin about the beginning of World War II are nonsense and pursue a purely pragmatic goal". Moreover the Molotov-Ribbentrop Pact "cannot be considered a military conspiracy between two dictators." (https://euvsdisinfo.eu/disinformation-cases/) Even more, for the Soviet and then Russian propaganda the WWII began on 22 June 1941, when Germany attacked the URSS and not on 1 September 1939, when Germany invaded Poland.

In this case the EU facts first approach is more than obvious. Eu vs. Disinfo experts choose to take act and promote the historical facts about the Molotov-Ribbentrop Pact. The agreement between Russia and Germany contained the Secret Supplementary Protocol[4], which assumed the invasion and the division of Poland and other Eastern European countries between the two military powers. Thus, the signing of the Molotov-Ribbentrop Pact led to German and Soviet military aggression against Poland in September 1939, which marked the beginning of the WWII. The Soviet Union attacked Poland on September 17, forcing the Polish army to fight on two fronts. Poland was divided according to the agreements of the Molotov-Ribbentrop pact. The USSR later attacked Finland and annexed the Baltic States and parts of Romanian territory, all as agreed in the pact with Nazi Germany.

[4] The secret protocol was about the delimitation of areas of mutual interest in Eastern Europe. In particular, Hitler and Stalin agreed to divide Poland. The agreement also indicated that the Baltic states of Latvia, Estonia and Lithuania, as well as Bessarabia and Finland, also belonged to the respective areas of interest of Germany and the USSR.

The myth of liberation. Soviet propaganda and now the Russian propaganda present Stalin as a liberator. According to Eu vs Disinfo specialists, "this case represents a manipulation of historical facts to downplay and justify Soviet aggression towards Poland, Finland, Baltic States and Romania". (https://euvsdisinfo.eu/disinformation-cases/) The facts presented are: Germany and the USSR invaded and divided Poland according to the agreements of the Molotov-Ribbentrop pact. USSR later attacked Finland. The Treaty enabled the Soviet Union to invade and annex the Baltic States. The Soviets also annexed Romania's provinces of Bessarabia (today's Moldova) and Herţa in the northern Bukovina (now in Ukraine) and the Czechoslovak territory of Carpathian Ruthenia (now also part of Ukraine). While the Red Army's contribution to the liberation of Poland is a fact, the results of the territory occupation are intentionally omitted. The Red Army's presence in Poland and in other Eastern Europe countries resulted in a setup of repressive communist regimes by the Soviet Union.

"The USSR tried to prevent the start of WWII, but Europe abandoned the anti-Hitler coalition". This is a typical case of manipulation of facts and propaganda narrative about the supposedly hostile anti-Russian intentions and policies of the aggressive West. The Russian propaganda state that the "Soviet side had to sign Molotov-Ribbentrop pact, which was a forced measure" when Great Britain, France, Poland and the USSR could not find a compromise to create a coalition. The fact is that during the so-called Moscow Negotiations, which began in May and lasted until August 1939, Poland categorically refused to let the Red Army on its territory, fearing Soviet occupation. But, the USSR also started negotiations with Germany in parallel and on August 23, 1939, signed the Molotov-Ribbentrop Pact (https://euvsdisinfo.eu/disinformation-cases/)

"**USSR was a victim of the Nazi and Polish aggression".** According to Soviet propaganda, "Poland was among those who initiated World War II. When Hitler came to power, the leader of Poland Pilsudski asked for an alliance with the Germans to march on Red

Square" (https://euvsdisinfo.eu/disinformation-cases/). Thus, USSR signed the Ribbentrop-Molotov Pact with Nazi Germany due to Poland's aggressive foreign policy. Historical documents released by Russia's Ministry of Foreign Affairs showed that the Soviet Union decided to sign the Ribbentrop-Molotov Pact with Nazi Germany for two reasons: 1) the aggressive foreign policy of Poland, which prevented a Soviet alliance with France and the United Kingdom, and 2) fears of an eventual Polish-German military alliance that would pose a really serious threat to the USSR. However, no evidence is provided to support the affirmation, it may be considered as part of the Russian efforts of historical revisionism, in order to portray Russia's role in World War II as a non-aggressive power and Poland as one of the main culprits of the conflict. Eu vs. Disinfo presents the fact: "It is true that several European powers, including Poland, signed non-aggression treaties with Germany in the 30s, but none of these treaties was as far-reaching as the Molotov-Ribbentrop pact, clearly dividing independent countries in Europe, Poland, Lithuania, Latvia, Estonia, Finland, and Romania, into *spheres of interests*". (https://euvsdisinfo.eu/disinformation-cases/)

Conclusions

State-sponsored disinformation has become an important tool of hybrid warfare weakening the European Union institutional framework and the democratic values, undermining the security architecture of Europe and spreading uncertainty. Experts state that "given its cross-border dimension, the adverse effects of disinformation in the European Union require a coordinated and long-term approach to respond to the challenge at both regional and national level."(MSB Report, July 2018)

According to EU official documents, the first and most important step is to recognise and expose Russian disinformation and propaganda activities by: "fact-checking through independent news organisations and civil society organisations – which is considered the method that better contributes to counter the spread of disinformation online; mapping and networking together independent fact-checking organisations in Europe and especially in the Black Sea Area, in order to advocate for a Black Sea fact-checking community; strengthening the

creation of an independent European network of fact-checkers to establish common working methods, exchange best practices and achieve the broadest possible coverage across the EU." (*Action Plan*, December 2018) Although the use of disinformation by state or non-state actors, especially by Russia, it is not quite new, the "EU contends that, since Russia's annexation of Crimea in 2014 and its subsequent role in the conflict in Eastern Ukraine, the Kremlin has accelerated its efforts to distort information being received throughout Europe." (*Action Plan*, December 2018)

Fake history is used in such disinformation campaigns promoting false narratives about the European past, misinterpreting, twisting, or omitting important key facts in order to present victims as oppressors and oppressors as victims. This is the WWII memories case, Europe being witness for the last two years to an unprecedented Russian historical revisionism. The means used for promoting fake history are multiple: "the Russian government has upgraded its international television news channel (RT), established a new global news agency (Sputnik), and reportedly targeted hundreds of European news outlets in an attempt to spread its disinformation" (Lucas and Pomerantsev, 2016).

In this paper, we highlight the Russian disinformation and propaganda cases about WWI and the Molotov-Ribbentrop Pact, all messages being part of the Kremlin's policy of historical revisionism and an attempt to portray Russia's role in World War II as non-aggressive. The EU *facts-first approach* is based on the idea that disinformation should be countered by ensuring that citizens have access to facts. Thus, the European approach suggests that fact-checking, debunking and deconstructing disinformation and fake history should constitute the core of countering disinformation and propaganda.

Annex
Disinformation cases about WWII and Molotov-Ribbentrop Pact
(Source: https://euvsdisinfo.eu/disinformation-cases/?text=&disinfo_issue=&date)

Case no.	Publication date	Disinformation	Source	Disproof
1.	06.07.2021	Europe insists on historical revisionism about World War II	sputniknews.gr	Recurring pro-Kremlin disinformation narrative **distorting the events** leading up to the Second World War and accusing the West of historical revisionism.
2.	27.06.2021	The West wants to rewrite World War II history	sputniknews.gr	The Kremlin's **campaign for historical revisionism on WWII** in order to boost its legitimacy and deny the USSR's responsibility in the outbreak of WWII.
3.	22.06.2021	European Union is spreading anti-Soviet myths about the beginning of World War II	baltnews.lt	The claim advances a recurring pro-Kremlin disinformation narrative **distorting the events** leading up to the Second World War, and accusing the West of historical revisionism.
4.	22.06.2021	Lithuania revises history since it interrupted the restoration of Soviet war monuments	sputniknews.lt, lt.sputniknews.ru	Recurring pro-Kremlin disinformation narrative **distorting the events**. Recurring disinformation about historical revisionism in Lithuania.
5.	22.06.2021	Myths, new interpretations, and fables about WWII are regularly composed in the West	ru.armenia sputnik.am, uz.sputniknews.ru, sputnik.by, lv.sputniknews.ru	The claim about the Western myths and fables about World War II is part of the Kremlin's **campaign on historical revisionism of WWII**.

6.	12.02.2021	The West has radically revised and rewritten WW2 history	eadaily.com	This message is part of the Kremlin's **campaign on historical revisionism of WWII** and is also consistent with recurring pro-Kremlin **propaganda narrative about anti-Russian policies of the aggressive West**.
7.	08.02.2021	Russia doesn't move outside the framework of international laws	akhbarak.net, alshbaka.net, RT Arabic, elbayan-news.com, eshraag.com, essahra.net, kachaf.com, kol-masr.com, lampress.net, msdernet.xyz, nabd.com, nafeza2world.com, newsformy.com, raialyoum.com, Sahafaty	The Kremlin's **campaign on historical revisionism of WWII** and is also consistent with recurring pro-Kremlin propaganda narrative about anti-Russian policies of the aggressive West.
8.	21.11.2020	The myth that victory in the WWII is the merit of the US	Sputnik Georgia	Recurrent pro-Kremlin disinformation on World War II **and historical revisionism,** accusing the West of rewriting history and trying to deprive Russia of its glorious victory over Nazi Germany.
9.	02.11.2020	Lithuania is fighting against the monuments of the Soviet army and re-writing history of WWII	Sputnik Lithuania, Sputnik Lithuania - Russian	This message is part of the Kremlin's policy and **campaign for historical revisionism.**

10.	24.09.2020	The aim of the Konev[5] Monument removal is to humiliate Russia and damage its prestige[6]	Ritm Evrazii	It is also consistent with common pro-Kremlin **disinformation narratives about Russophobia** and the supposedly hostile anti-Russian intentions of the West, based on which Russia can cast itself as the victim.
11.	18.09.2020	In September 1939 the USSR did not attack Poland, but carried out the liberation campaign of the Red Army	regnum.ru	This is a pro-Kremlin **narrative about Russophobia** and a clear case of **historical revisionism about WWII.**
12.	04.09.2020	The Munich agreement started World War II	politnavigator.net	This is a pro-Kremlin **conspiracy narrative about WWII** and the Munich Agreement.
13.	03.09.2020	Accusing USSR of WWII outbreak, Poland distracts attention from its pre-war "miscalculations"	Sputnik Poland	This message is part of the Kremlin's **policy/ campaign for historical revisionism** and an attempt to erode the disastrous historical role of the Molotov-Ribbentrop Pact and to **reject the historical fact of the Soviet attack** at Poland in September 1939.

[5] Marshall Konev led the Red Army forces that liberated Prague and large parts of Czechoslovakia from the Nazi occupation in 1945. His monument, unveiled in the Prague 6 district in 1980 when the country was occupied by Soviet troops, has been a source of controversy.

[6] A worker covered the statue of a Soviet World War II commander Marshall Ivan Stepanovic Konev after its removal from its site in Prague on April 3, 2020. See more on *Russia Aims to Prosecute Destruction of War Monuments Abroad*, Associated Press, Moscow, April 8, 2020, accessible on https://www.usnews.com/news/world/articles/2020-04-08/russia-aims-to-prosecute-destruction-of-war-monuments-abroad

14.	01.09.2020	Europe is to blame for the outbreak of World War II	Pervyi kanal	This is a pro-Kremlin narrative and a clear case of **historical revisionism about WWII.**
15.	01.09.2020	Poland euphorically re-writes the history of WWII, spreading Russophobia	Sputnik Poland	The Kremlin's **policy of historical revisionism** – it accuses Poland of the "falsification and re-writing" of WWII history. It is also consistent with common pro-Kremlin **disinformation narratives about Russophobia**
16.	23.06.2020	The Munich Agreement began World War II	News Front - Russian, ria.ru	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism about the WWII** and the Munich Agreement.
17.	19.06.2020	USSR did its utmost to create anti-Hitler coalition, the West left it to deal with Nazi Germany alone	Sputnik Italia	Recurring pro-Kremlin disinformation narrative **distorting the events** leading up to the Second World War
18.	19.06.2020	The Munich Agreement triggered World War II	Sputnik Italia	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism** about the WWII and the Munich Agreement.
19.	13.05.2020	Poland reached mutual Agreement with Nazi Germany and participated in the partition of Czechoslovakia after the Munich Pact	Sputnik Italia	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism about the WWII** and the Munich Agreement.

20.	08.05.2020	Western media try to minimize Soviet victory in WWII	Ahí les Va - YouTube	This is a pro-Kremlin **conspiracy narrative about WWII and the West intentions.**
21.	29.02.2020	Europe justifies the Munich Agreement with Hitler	Rossia 24 - YouTube	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism about the WWII and the Munich Agreement**.
22.	06.02.2020	Poland is largely responsible for WWII	Spuntik Polska	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
23.	28.01.2020	Calling German-Soviet non-aggression pact as Ribbentrop-Molotov pact is re-writing history	Sputnik Polska	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism about the WWII** and the Munich Agreement.
24.	14.01.2020	Nazi-Soviet Non-Aggression Pact was a direct result of British, French and Polish politics	Sputnik Polska	This is a pro-Kremlin **conspiracy narrative about WWII and the West intentions.**
25.	01.10.2019	The resolution of the European Parliament shows that Europe has become insolent	Sputnik Srbija	This is a pro-Kremlin **conspiracy narrative about WWII and the West intentions.**
26.	01.10.2019	The Munich Agreement triggered WWII and the USSR was completely ignored	Sputnik Deutschland	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism about the WWII and the Munich Agreement**.
27.	09.09.2019	The USSR signed the Ribbentrop-Molotov Pact with Nazi Germany due to Poland's	Sputnik Mundo	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism about the WWII and the Munich**

		aggressive foreign policy		**Agreement**.
28.	05.09.2019	WWII commemorations in Poland: Non-invitation of Russia is NATO information campaign	Sputnik Deutsch	**Conspiracy theory** consistent with recurring pro-Kremlin narratives about the West's anti-Russian actions
29.	05.09.2019	The Soviet Union was forced to sign the Molotov-Ribbentrop Pact	Sputnik Srbija	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism** about WWII and Molotov-Ribbentrop Pact
30.	01.09.2019	US ordered the start of the World War II to defeat Britain	Tsargrad TV	**Conspiracy theory**, no evidence given. This is one of the pro-Kremlin disinformation narratives about the WWII
31.	01.09.2019	The Molotov-Ribbentrop Pact played no role in unleashing World War II	strana.ua	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
32.	01.09.2019	USSR was not an aggressor in World War 2, it was forced to sign the Molotov-Ribbentrop Pact	riafan.ru	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
33.	01.09.2019	Poland is responsible for the unleashing of World War II	Voskresnyi vecher s Vladimirom Solovyoivym @ Rossiya 1	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
34.	01.09.2019	Poland is the organizer of WWII and its main culprit	Voskresnyi Vecher s Vladimirom Solovyovym @ Rossiya 1	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism** about WWII and Poland's role in the WWII

35.	01.09.2019	Poles killed more than 400,000 Jews during WWII	Voskresnyi Vecher s Vladimirom Solovyovym @ Rossiya 1	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism** about WWII and Poland's role in the WWII
36.	01.09.2019	The Soviet Union saved Poland from ruin after WWII	Voskresnyi Vecher s Vladimirom Solovyovym @ Rossiya 1	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
37.	30.08.2019	WWII anniversary: The events in Poland are an anti-Russian gathering	Vremya Pokazhet @ Pervyi Kanal	**Conspiracy theory** consistent with recurring pro-Kremlin narratives about the West's anti-Russian actions
38.	26.08.2019	Russia was not invited to events commemorating WWII because of anti-Russian politics	Russian RT	This is a pro-Kremlin **narrative about Russophobia** and a clear case of **historical revisionism about WWII.**
39.	23.08.2019	Polish nationalists are trying to refute evidence on Poland's role in unleashing the Second World War	South Front	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
40.	23.08.2019	The Baltic States benefited from the Molotov-Ribbentrop pact	60 Minut @ Rossiya 1	This claim uses historical revisionism to reinforce common pro-Kremlin disinformation narratives about WWII and the Molotov-Ribbentrop pact.
41.	23.08.2019	If Poland realized a rational policy in 1939, Moscow would have had a different approach towards it	Sputnik Polska	This case represents a **manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
42.	22.08.2019	Signing of the Molotov-	Sputnik Polska	This case represents a **manipulation of**

		Ribbentrop Pact thwarted the UK's expansionist plans in Europe		**historical facts** to downplay and justify Molotov-Ribbentrop Pact
43.	20.08.2019	Soviet Union was forced to sign the Molotov-Ribbentrop Pact	RIA Novosti	This case represents a **manipulation of historical facts** to downplay and justify Molotov-Ribbentrop Pact
44.	13.08.2019	The Molotov-Ribbentrop Pact is being demonized by the European countries	Baltnews	This case represents a **manipulation of historical facts** to downplay and justify Molotov-Ribbentrop Pact
45.	13.08.2019	USSR was forced and reluctant to sign Molotov-Ribbentrop Pact	Baltnews.ee	This case represents a **manipulation of historical facts** to downplay and justify Molotov-Ribbentrop Pact
46.	11.08.2019	The Munich conspiracy of European powers launched the WWII	Baltnews	This is a pro-Kremlin **conspiracy narrative** about the WWII
47.	11.08.2019	The Molotov-Ribbentrop Pact did not trigger World War II. Russia was threatened by Germany	Baltnews	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism** about WWII and Poland's role in the WWII.
48.	01.08.2019	Poland re-writes the history of the Warsaw Uprising accusing the USSR of its failure	Sputnik Polska	This is a **conspiracy theory** about the WWII
49.	26.07.2019	Poland did not invite Putin to the WWII commemoration ceremony to disrupt Belarus-Russia relations	Grani Formata @ Sputnik Belarus	**Conspiracy theory** consistent with recurring pro-Kremlin narratives about the West's anti-Russian actions and attempts to discredit and disrupt Belarus-Russia relations

50.	24.07.2019	Due to the alleged aggression in Crimea, Russia was not invited to the anniversary of the beginning of World War II	Sputnik Serbia	**Conspiracy theory** consistent with recurring pro-Kremlin narratives about the West's anti-Russian actions
51.	23.07.2019	Poland wanted to ally with Germany and attack the USSR	Sputnik Estonia	This is a **conspiracy theory** about the WWII and **manipulation of facts.**
52.	23.07.2019	The Molotov-Ribbentrop Pact did not violate the rights of the Polish state	Sputnik Polska	This message is part of the Kremlin's **policy of historical revisionism** and an attempt to portray Russia's role in the World War II as not aggressive.
53.	22.07.2019	Stalin decided to establish the independent Polish state	Sputnik Polska	This message is part of Russian **historical revisionism** and part of a disinformation campaign portraying Russia as the peace-maker and liberator.
54.	17.07.2019	The USSR tried to prevent the start of WWII, but Europe abandoned the anti-Hitler coalition	Rg.ru	This message is part of **Russian historical revisionism** and part of a disinformation campaign portraying Russia as the peace-maker and liberator.
55.	15.07.2019	The Baltic States are perpetuating the myth of the Soviet occupation	Rubaltic.ru	This message is part of Russian **historical revisionism** and part of a disinformation campaign portraying Russia as the peace-maker and liberator.
56.	05.07.2019	Poland wants Belarus to return the property of Second Polish Republic	Imhoclub.by, Sozh.info, BelVPO	This is a **conspiracy theory** about the Polish political intentions.

57.	04.07.2019	USSR is not to blame for the beginning of World War II	Pravda.ru	This message is part of **Russian historical revisionism and** part of a disinformation campaign portraying Russia as the peace-maker and liberator.
58.	04.07.2019	USSR was not going to divide Poland	Sputnik Armenia	This is a pro-Kremlin narrative which is itself a clear case of **historical revisionism** about WWII.
59.	16.06.2019	It is thanks to Russia that Poland today exists as a country	Tolstoy @ Pervyi Kanal	**A distorted, unfounded comparison** between NATO and Russia as ''guaranteeing security'' of Poland
60.	13.06.2019	Russia signed Molotv-Ribbentrop pact because it was threatened by Germany. Today Russia is threatened by Poland.	Vremya Pokhazet @ Pervyi kanal	This case represents a **manipulation of historical facts** to downplay and justify Molotov-Ribbentrop Pact.
61.	13.06.2019	Russia has given Poland its independence	Vremya Pokhazhet @ Pervyi Kanal	**Manipulation of historical facts** to downplay and justify Soviet aggression towards Poland.
62.	06.06.2019	The Russian delegation was not invited to the 80th anniversary of the outbreak of World War II because of the Russian ban on the imports of Polish apples	Teleskop, http://teleskop-by.org/	This is a **conspiracy consistent** with recurring pro-Kremlin narrative about the West's anti-Russian actions.
63.	21.05.2019	Russia opposes any attempts to "destroy the post-	Vremya @ Pervyi kanal	This case represents a **manipulation of historical facts** to

		WWII security architecture"		downplay and justify Molotov-Ribbentrop Pact.
64.	21.05.2019	Only thanks to Stalin did Poland receive the German Danzig (Gdansk)	Sputnik Armenia	This message is part of **Russian historical revisionism** and part of a disinformation campaign portraying Russia as the peace-maker and liberator.
65.	09.05.2019	Western powers try to keep Soviet victory over Nazi Germany in the dark	Sputnik Spanish	**Conspiracy theory** consistent with recurring pro-Kremlin narratives about the West's anti-Russian actions

References:

1. *A Multi-dimensional Approach to Disinformation. Final Report of the High-Level Expert Group on Fake News and Online Disinformation.* European Commission. (30 March 2018). Available online on https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

2. *April Communication of European Commission. Tackling online disinformation: a European Approach*, Brussels, 26.4.2018 COM (2018) 236 final. Available online on http://www.europarl.europa.eu/resources/library/media/20180926RES14426/20180926RES14426.pdf

3. Bayer, Judit, Bitiukova, Natalija, Bárd, Petra, Szakács, Judit, Alemanno, Alberto, Uszkiewicz, Erik, (February 2019). *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, Directorate General for Internal Policies of the Union. Available online on http://www.europarl.europa.eu/committees/en/supporting-analyses-search.html

4. European Parliament, *Understanding propaganda and disinformation*, November 2015.

5. European Parliament Resolution of 23 November 2016, *EU strategic communication to counteract anti-EU propaganda by third parties*, Strasbourg. Available online on http://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.pdf

6. *European leaders call for continued and coordinated efforts to counter disinformation threats,* 22/03/2019. Available online on https://eeas.europa.eu/headquarters/headquarters-homepage/60089/european-leaders-call-continued-and-coordinated-efforts-counter-disinformation-threats_en

7. Funke, Daniel, (2018). *A guide to anti-misinformation actions around the world*, Poynter, July 2. Available online on https://www.poynter.org/news/guide-anti-misinformation-actions-around-world

8. Giles, Keir, (March 2016). *Russia's 'New' Tools for Confronting the West. Continuity and Innovation in Moscow's Exercise of Power*. Available online on https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf

9. Graves, L., Cherubini, F. (2016). *The rise of fact-checking sites in Europe*. Reuters Institute for the Study of Journalism, available on-line on https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Rise%2520of%2520FactChecking%2520Sites%2520in%2520Europe.pdf.

10. Jack, Caroline, (2017). Lexicon of Lies: Terms for Problematic Information, Data & Society Research Institute. Available online on https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf

11. *Joint declaration on freedom of expression and "fake news", disinformation and propaganda*, (2017). Available online on https://www.osce.org/fom/302796

12. *Joint Statement by Estonia, Latvia, Lithuania, Poland and Romania on the occasion of 80 years since the signing of Molotov-Ribbentrop Pact*, 23 August 2019. Available online on https://www.gov.pl/web/diplomacy/joint-statement-by-estonia-latvia-lithuania-poland-and-romania-on-the-occasion-of-80-years-since-the-signing-of-molotov-ribbentrop-pact

13. Lange-Ionatamišvili, Elīna, (2016). Resisting Foreign State Propaganda in the New Information Environment: the case of the EU, Russia, and the Eastern Partnership countries, NATO Strategic Communications Centre of Excellence. Available online on http://appc.lv/wp-content/uploads/2016/09/Propoganda_petijums.pdf

14. Lucas, Edward, Pomerantsev, Peter (2016). Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe, CEPA.

15. Marek Ney-Krwawicz, *The Polish Underground State and The Home Army (1939-45).* Available online on http://www.polishresistance-ak.org/PR_WWII_texts_En/02_Article_En.pdf

16. Marwick, A., and Lewis, R. (2017). *Media Manipulation and Disinformation Online* [whitepaper]. New York: Data & Society Research

Institute. Available online on https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

17. Milo, Daniel, Klingová, Katarína, (2016). *Countering information war. Lessons learned from NATO and Partners Countries*, GLOBSEC Policy Institute.

18. Oh, Sarah, Adkins, Travis L., (June 2018). InterAction Disinformation Toolkit. Available online on https://www.interaction.org/documents/disinformation-toolkit/

19. *Questions and answers about the East StratCom task force*. Available online on https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

20. Špalková, Veronika, (2018). *Influence of Russian disinformation operations: specific examples in data and numbers*, Kremlin Watch Program.

21. Stencel, Mark, Griffin, Riley, (2018). *Fact-checking triples over four years*, ReportersLab, February 22. Available online on https://reporterslab.org/fact-checking-triples-over-four-years/?print=true

22. *The Prague Manual, (2018).* Kremlin Watch Report. European Values Think-Thank Team, Prague.

23. Wardle, C., Derakhshan, H. (2018). *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI (2017)09, 2017. Available online on https://rm.coe.int/information-disorder-report-november-2017/1680764666)

24. *What is fact checking and why is it important?* (18 November 2018). Available online on https://factcheckni.org/blog/what-is-fact-checking-and-why-is-it-important/and https://coinform.eu/what-is-fact-checking-and-why- is-it-important/

25. Disinformation cases. Available online on https://euvsdisinfo.eu/disinformation-cases/

NEW MEDIA: ANYONE, ANYWHERE & ANYTIME

Raluca MUNTENIȚĂ*

Abstract:
In its processes of creating and disseminating news, the media aims to satisfy the public's needs for information and knowledge as well as entertainment. Beyond the traditional publication of news via traditional media such as print, radio or television, the new trend is accessing news online. Blogs, forums, social networks and search engines are all environments in which information is becoming increasingly visible, increasingly accessed and increasingly read. Warts and all: these means are defined by a series of characteristics, but they also conceal certain dangers: ideological polarization, filter bubbles, selective exposure etc.

Keywords: *Internet, old media, new media, blogs, forums, social platforms, citizen journalism*.

Introduction

Beyond the classical dissemination of news through traditional channels – newspapers, radio, and television – news began to be increasingly visible and accessed online after *the advent of the Internet* which significantly changed the communication environment by introducing new communication channels: e-mail, online publications, websites etc. Moreover, the Internet fostered interaction between people and technology; that technology was not completely new, it already existed, but through creative ways of using it, technology attracted public attention.

If 30 years ago Romanians had access to radio and television services at certain times of the day, today the Internet – the gateway to

* PhD Student, National School of Political Science and Public Administration, email: ralucamuntenita@yahoo.com

an unlimited volume of information (text, image and sound) – facilitates rapid and relatively low-cost interaction between two or more people, regardless of their geographical location. The Internet brings people together, creates the space for them to communicate regardless of the time of day, facilitates the exchange of ideas, opinions, experiences, photos, helps them sell or buy etc.

Without a standard definition, *new media* refers to those technologies that already exist, but which have acquired high popularity through the creativity of their users. Whether we refer to blogs, social networks or citizen journalism, *new media means new world*, where information online becomes more visible, more accessed and more read than in print. *New media offers a different perspective* on news, where the subject of interest can be known and understood without the journalist's presence and where the news consumer has full power to intervene at any time to make his or her opinion known. They can (dis)agree on a particular subject or issue of domestic or international interest at one click distance, using all the means at their disposal – reaction, comment, share.

New media – understood as means of communication via the Internet – thus refers to traditional online media and social media, also called vertical and horizontal online communication channels. While vertical channels define traditional media based on a hierarchical structure (which implies the existence of journalists), horizontal channels refer to social media which allows the combination of the roles of producer-consumer/sender-receiver of information (McCombs, 2014).

New Media: advantages and disadvantages

One of the main defining characteristics of new media refers to *the ability* of individuals *to operate*, in their own name, *with an impressive volume of information* and to pass it through all stages: collection – storage – processing – filtering – dissemination.

Other characteristics include: *interactivity*, which makes it easy to manipulate, select, link and distribute the data and information; *connectivity* (thanks to search engines and social networks); *density* of information; *variety*, through the unlimited supply of information;

spontaneity; *decentralisation* (as opposed to the old media, which relied on a publisher, radio or TV broadcaster etc.); *dual role* (the consumer of information can become its producer at any time); *free access* (an individual can access and use any information or communicate via a blog, forum or social network at any time, from anywhere); *feedback* (unlike the limits imposed by old media, an individual can now express his or her opinion on a subject at any time); *spatial limitation* (in the Internet environment, any cultural/social/ etc. barriers disappear); *cost reduction* (whereas in the old media era, the whole process of collecting – processing – disseminating information required a premises, a distribution system, a studio and radio or TV equipment, in the new media era, the colossal amount of digital content requires a computer and access to the Internet); *active participation* (involving a theoretically unlimited number of people); *simultaneous communication* on several digital media (Gane & Beer, 2008).

Thus, under the new conditions, an individual can choose *to react* (positively or negatively) to an already existing piece of information, but also has the possibility to create content himself (on a blog or on a personal account from a social network), *to disseminate* it and to wait for reactions (likes, comments or shares) from those who follow him or her. In turn, his or her followers have the opportunity (which is not guaranteed by old media) to react to the content posted, through feedback, in line with their own beliefs, anytime and anywhere. A significant number of people *can interact and engage* in different actions at the same time thanks to the new means of communication.

Moreover, in recent years, there has been a growing trend for publications, radio and television stations, public institutions and private companies, personalities and individuals to go online using websites and social platforms. Anyone can live now in the virtual environment and can be contacted by anyone, anytime, anywhere.

On the other hand, given that the online environment gives the consumer control over the content they host, it should not be forgotten that they can also ask for something in return.

Some of the disadvantages that new media come with can be: a continuous information cycle that generates an endless flow of information *can become stressful* for the consumer; the sources that

disseminate content *become more important* than those that process and filter it; the consumer might become *trapped in a filter bubble* where he is "fed" only with the information he uses and accepts, thus ignoring other opinions and other realities; *control* over what is disseminated *can easily be lost*, as the person creating content in online does not necessarily need a minimal training or studies in the field; as a result, *distrust of content* published online *can increase* (lack of filters allows misleading content to circulate freely); *clickbait culture* can be amplified by content with sensational or bombastic headlines, full of superficial information, poorly documented or intentionally invented (Kovack & Rosenstiel, 2001).

Viewed in opposition, the two media – *old and new* – differ, as might be expected, on several levels: homogeneity vs. heterogeneity (while old media is defined by a unitary structure, new media advocates diversification of media); centralization vs. decentralization (old media is solidary in terms of the content disseminated and serves as a catalyst for public discussion, while new media have fostered the development of numerous groups of individuals with their own specificities and interest in only a few topics); local vs. global (while old media is theoretically limited to the language, culture and events of a single city or state, new media presents events and allows reactions from all over the world, in all languages); limited vs. unlimited (even if old media offers diverse content, this cannot be compared to what new media provides); passive vs. active (while old media requires passive attendance to what they present, new media encourages and allows free expression) (Monosson, 2005).

At the same time, other differences between these two are obvious in terms of: *transparency* (while old media sets the degree of transparency, new media extends its limits; *dissemination* (old media processes and distributes information, new media gives freedom to individuals to create and post content of any kind); *freedom* (old media activity is regulated by law and takes into account certain ethical standards, while new media activity does not feel constrained at the moment); *autonomy* (old media is characterized by a hierarchical structure, new media promotes the individual imprint of users); *influence* (whereas in the centralized hierarchy of old media the

authority lies with the company or agency producing and disseminating information, in new media anyone is free to exert influence on anyone) (Jodoin, 2014).

On the other hand, the relationship between the two media can be characterized by three phenomena: competition, complementarity and integration (Neuberger, 2010). Competition is the rivalry created between the two media in the rush to increase popularity and attract advertisers. Complementarity plays a significant role as content writers are rather attracted not by the major issues themselves, but by highlighting some of the issues they generate. Integration takes place through the reciprocal use of media as a source of information.

In the context of new media, we are talking about the generation gap and the difference between individuals born before the launch of new media (for whom this represents a technological boom) – *digital immigrants* (Palfrey & Gasser, 2008) or *baby boomers* (Tapscott, 2009) and individuals born after this technological boom (for whom new media is natural) – *digital natives* (Palfrey, 2008) or the *Net Geners* (Tapscott, 2009).

Clearly, this difference between the two generations is nothing new. What is striking, however, is the peculiarity that individuals of the first generation tend to borrow, consciously or unconsciously, from the behaviours exhibited by individuals of the new generation. Thus, often, adults are those who learn from their children how to enjoy the benefits of new media.

New media has the greatest influence on young people, involving them in all the activities they cover. Whereas the old media told individuals what information to consume, the new media leaves all freedom to the consumer (they can choose and process any information themselves), which is particularly important given that "the Net Geners don't just take what they are offered. They are initiators, organizers, readers, writers (...). They don't just observe they participate. They research, debate, play, critique, investigate, ridicule, search and inform" (Tapscott, 2009, p. 21).

New Media, New Challenges

Changes produced in the media, including the expansion of the Internet, also involve a number of challenges for agenda-setters as mass communication (known in its classical sense) is transformed into multi-channel mass communication.

Several factors have contributed to the *hybridization of media systems*: the new role given to the information consumer (who can now act as both author and recipient of information); new ways of using the media available to the consumer; changes in the way programs are transmitted; and the diversification of types of media communication. The *reversal of producer-consumer roles* may also lead to a scenario where the media may no longer be able to set the public agenda and will therefore be forced to obey it. Such changes are based not only on the process of hybridization, but also on the (increasing) commercialization of media content.

Competition (mentioned above) may be a good reason for more and more content producers to focus first and foremost on meeting the knowledge needs of their consumers (e.g., see the media's appetite for providing considerably more soft news at the expense of hard news when it comes to public policy). This situation quickly translates into a challenge for agenda-setting theory, if we consider that the return to consumer needs implies that the activity of selecting topics for the media agenda should be decided, as appropriate, by readers, viewers, internet users (as consumers) and not, as hitherto, by accredited journalists (as producers). The likelihood of reverse agenda-setting (where the public agenda affects the media agenda) (Weimann & Brosius, 2016) can also be attributed to the growing interest in increasing audiences and earnings.

Today, various profile agencies are monitoring the activity of search engines, blogs, forums and social platforms to track what issues are of interest in order to develop new topics, designed not only to get consumers' attention, but also to get them to react according to their own beliefs - to provide feedback (Ragas et al., 2014). Media research and the ranking of topics according to audience preferences greatly affects the structure set by the media agenda.

As a result, new agendas are identified: in addition to the real-world agenda, the agenda of blogs, forums, social networks or search engine queries have been highlighted. While the real-world agenda is known to be composed of major issues that are part of the immediate reality and are distinguished by socio-economic-political indicators (unemployment, climate change, protests, etc.), the online agendas are composed of roughly the same topics, but the importance given to each leads to a different ranking.

The development of new media has brought blogs, forums and social platforms into the online space (and, also, bloggers and users of forum or social network accounts). As public journals (blogs), spaces for discussion (forums) or complex activities (social networks), they all offer great freedom of expression and exposure in the virtual public space.

For example, a blogger/social networker can act as an early warning or opinion leader. These types of people are of importance either because they are recognized as representatives of the public, or because they are representatives of the media, or because they are representatives of the political agenda (if we think that behind a blog or an account there can be an ordinary citizen, a journalist, a celebrity, a political personality etc.). The topics that such a person highlights at a given time as being of interest can then be picked up, publicized and debated by accredited journalists. And this happens. By communicating directly with the public, many bloggers or social media users have become much better known, followed and read than well-established journalists. This is where the dual nature of the citizen, who consumes content while becoming a content producer himself, comes in. This phenomenon has been a turning point in journalism: many journalists have chosen to reach out to the public via a blog or an official Facebook/Twitter/Instagram page, thus jumping over the editorial barrier.

Citizen journalism is that activity undertaken by ordinary amateur citizens who have no journalistic training, but who generate media content about breaking news events or other types of news (Blaagaard, 2013). The chance to be in a certain place at a certain time, where a certain event – earthquake, flood, accident, explosion, protest etc. – is taking place, can turn them from ordinary citizens into

occasional journalists. Today, any individual who owns (at least) a mobile phone and witnesses an event (with impact on society) can record, take pictures or do live sessions from the scene. Moreover, the person concerned, as a witness, can also provide some information – an account of what happened – about the event in question. Breaking news is the most common occasion when anonymous citizens – who become "accidental" bystanders (Harrison, 2010, p. 245) – share images, footage or testimonies with their peers via social networking accounts and groups, video-sharing platforms, free messaging apps etc.

What is important to note here, however, is that not all such photo and/or video material can be labelled as citizen journalism? To talk about this type of journalism, it is necessary for the citizen to play an active role in all steps of the process: capturing the information (photo/video), analysing it (through its own filter as the witness to the experience) and disseminating it on the various platforms; in other words, it is the citizen who is responsible for all the steps involved in the process of making a news story.

These conditions *differentiate citizen journalism from participatory journalism*, where there is collaboration between the citizen-witness and the journalist. In this case, a photo or video of a person/event, which is taken by a citizen – witness, is then provided to journalists. Many domestic and international media companies have understood the importance of this type of journalism (cost-effective – it is much cheaper and more efficient to create content from incoming photos or recordings than to send teams on the ground) and have created dedicated contact details and spaces for this type of content: *iReport* (CNN), *uReport* (Fox News), *Your news* (BBC) etc.

As far as citizen journalism is concerned, *three key-elements* need to be mentioned: a) information about the event was acquired through the use of low-cost tools (mobile phone, camera etc.); b) information about the event was freely published on interactive platforms (blogs, forums, social networks etc.); and c) the distribution of information was not mediated by another entity. The new paradigm transports us into an atypical informational zone, where content is created, recreated and distributed in such a way that it breaks the traditional pattern of consumption (Suárez-Villegas, 2017).

The establishment of an *intermediate agenda*, materialising between the traditional media agenda (journalists) and that of the new opinion formers (bloggers or social media individuals), would mean that journalists use blogs or social accounts as sources of information (thus giving them legitimacy) and the latter would rely on traditional media as sources of information. And, in this way, a cycle of news sources would be created, where news content is sent for "resurrection" from one medium to another: traditional media launch a story, online opinion leaders pick it up and popularise it, and then return it to the first sender to be debated as a trending topic.

On the other hand, the type of *agenda based on search engine queries* could also affect the media agenda. This type of agenda is seen as relevant to public opinion all the more so as human search behaviour here is both natural and independent (Ragas et al., 2014). Given that individuals use search engines in an individual and anonymous manner, the query-based type of agenda may reflect the public's desire for knowledge much more accurately than it would be reflected, for example, through opinion polls.

The implications of the relationship between old media and new media have also fostered the emergence of the concept of *agenda-melding*, which merges elements from different agendas into a personal agenda of a recipient or community and allows for the creation of a personalised picture of the world (Shaw & Weaver, 2014). The realisation of an individual or group agenda can (also) be determined by their socio-political preferences.

On the other hand, the development of new technologies can also result in "the amplification of various types of disinformation in circulation", which pose potential risks to democracy, national security and society (HLEG, 2018, p. 10). The phenomenon of disinformation is already a major challenge for journalists, who are now caught up in a vast process of checking and sorting the information to be disseminated to the public. The move of newspapers from offline to online and the consequent job cuts in the industry are contributing significantly to the degradation of journalism. Together, all this paves the way for another phenomenon: *fake news*.

Conclusions

In the absence of a standard definition, new media is represented by those technologies that already exist, but have gained notoriety through the creative ways in which they have been used by individuals. Blogs, forums, social networks or search engines – new media – are environments in which information becomes increasingly visible, increasingly accessed and increasingly read. All of these are defined by a series of characteristics – interactivity, connectivity, variety, spontaneity, free access etc. – but they also conceal certain dangers: ideological polarization, filter bubbles, selective exposure etc. Old and new media differ on several levels: homogeneity vs. heterogeneity, centralization vs. decentralization, transparency, autonomy, influence etc.

The emergence of blogs, forums or social platforms in the online space today offers wide freedom of expression and a high degree of exposure. A blogger/influencer on a social network becomes – thanks to the number of followers – much better known, followed and accessed than journalists or well-established media sources.

References:

1. HLEG. *A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation*, European Commission. Luxemburg: Publication Office in the European Union, 2018.

2. Blaagaard, B. B. (2013). "Shifting boundaries: Objectivity, citizen journalism and tomorrow's journalists", *Journalism*, no. 14, p. 1076–1090.

3. Gane, N., & Beer, D. (2008). New Media. New York: Berg.

4. Harrison, J. (2010). "User-generated content and gatekeeping at the BBC hub", *Journalism Studies*, no. 11(2), p. 243-256.

5. Jodoin, S. (2014). "Promesses et périls des nouveaux médias. Essai sur la médiasocialisation", in *Mutations de l'univers mediatique. Medias traditionels et nouveaux*. Quebec: Mediteur.

6. Kovach, B., & Rosenstiel, T. (2001). *The Elements of Journalism*. New York: Crown Publishers.

7. McCombs, M. (2014). *Setting the Agenda: Mass Media and Public Opinion. Second Edition*. Cambridge: Polity Press.

8. Monosson, R. 2005. *A New Audience for New Media*. Available from: www.webprofesion.com.

9. Neuberger, C. (2010). "Competition, Complementary or Integration? The relationship between professional and participatory media", *Journalism Practice*, no. 4(3), p. 319-332.

10. Palfrey, J., & Gasser, U. (2008). *Born digital: Understanding the first generation of digital natives*. New York: Basic Books.

11. Ragas, M., W., et al. (2014). "Media-Induced or Search-Driven? A study of online agenda-setting effect during the BP oil disaster", *Journalism Studies*, no. 15(1), p. 48-63.

12. Shaw, D. & Weaver, D. (2014). "Epilogue. Media agenda-setting and audience agenda-melding", in M. McCombs, *Setting the agenda. The mass media and public opinion*. Second edition, Cambridge: Polity Press.

13. Suárez-Villegas, J. C. (2017). "Citizen Journalism. Analysis of opinions of journalists from Spain, Italy and Belgium", *Convergencia – Revista de Ciencias Sociales*, no. 74, p. 91-111.

14. Tapscott, D. (2009). *Grown up Digital: How the Net Generation Is Changing the World*. New York: McGraw Hill.

15. Weimann, G., & Brosius, H. B. (2016). "Agenda-setting in the online Era", *The Agenda Setting Journal*, no. 1(1), p. 63-101.

GAMES, EXERCISES AND SIMULATIONS

FUTURE TRENDS EXERCISE. FRACTURED DIGITAL FUTURES: AI IN SERVICE OR AGAINST DEMOCRACIES? SOLUTIONS AHEAD

Valentin STOIAN-IORDACHE*
Cristina IVAN*
Alexandra ANGHEL*
Mihaela TEODOR*

Introduction

The following exercise scenario is based on the "Futures Frequency" methodology developed by the Finnish think-tank SITRA (Finnish Innovation Fund)[1], which employs it in order to establish possible future scenarios with the help of experts in the field. It was played during the Workshop, *Fractured Digital Futures: AI in Service or Against Democracies? (*September 2, 2021, Bucharest, Romania) within the Security in the Black Sea Region: Shared Challenges, Sustainable Future Program.

It includes three stages:

1. Challenging assumptions about the future
2. Imagining future scenarios

* Researcher PhD, National Institute for Intelligence Studies, MVNIA, email: stoian.valentin@animv.eu
*Researcher PhD, Head of National Institute for Intelligence Studies, MVNIA, email: ivan.cristina@animv.eu
* PhD Student, University of Bucharest and Researcher, National Centre for Modeling and Simulation in Intelligence, MVNIA, email: popescu.alexandra@animv.eu
* Senior Researcher PhD, National Centre for Modeling and Simulation in Intelligence, MVNIA, email: teodor.mihaela@animv.eu

[1] SITRA, Futures Frequency. Retrieved from https://www.sitra.fi/en/projects/futures-frequency/, Accessed 9.08.2021.

3. Action – establishing the steps we need to take in order for the imagined future to occur.

While this type of exercise can focus on numerous topics, or can discuss more topics in a single session, the particular exercise we will carry out today will focus on the overarching theme of *Fractured Digital Futures: AI in service or against democracies? Solutions ahead.*

Core themes

The exercise will focus on the following core themes:

1. How will the development of AI affect democracy, free speech and elections?

2. Will AI-enhanced education bring about a better cognitive development or will it make it more difficult to grasp abstract ideas?

3. How will medicine look like once AI is part of our life? Will we still become sick and die? Will human security be affected?

4. Will we live on a healthier planet? How will AI help with energy consumption and combating climate change? How will these developments impact state and global security?

5. Will we travel farther faster? How will AI help with the planning and security of transportation?

Stages – the exercise will proceed through the following stages:

Stage 1: The "What if?" stage – 20 minutes – Full Assembly

At this stage, all participants will be assembled in the main hall and will work together as one single, large, group. The moderator will ask participants to imagine a radical change about the mid-term future (ex. 2050) and to write it on a post-it in the form of a "What if?" question. However, given the topic of the overall workshop, participants should focus on possible changes brought about by the development of Artificial Intelligence, rather than about general topics. For example, one could ask himself/herself

- What if the medical profession would cease to exist, being replaced by medical robots? Will this affect decisions about who lives and who dies?

- What if drastic climate change will lead to robots regulating artificial closed environments where the financial, political and scientific elite will continue to form a small global society? Will these communities live in artificially created ecosystems, while the disenfranchised will struggle to survive in a chaotic outcast world?
- What if global decisions get to be taken by statesmen based on the algorithmic calculations and predications of the AI that is too complex for the human mind to grasp? Can humans still ensure self-governance?
- What if some individuals have died due to AI decisions in inevitable car accidents? AI has calculated which route variant implied a lesser number of victims, and that should be enough!

The goal of this initial step is to get everyone to think creatively about the future. This will represent the basis for the next stage, in which participants will be asked to challenge their assumptions about the future.

Stage 2: Challenging assumptions – 40 minutes – Small groups of 5-8 individuals

At this stage, the assembly will break up into small groups of 5-8 people each. Each of these groups will receive a pre-designed "vignette", a small story about a possible future. The five stories elaborated will each address how the evolution of artificial intelligence will impact a particular field of human activity: politics and democracy, education, medicine, transportation, climate and energy, and how each of these will affect the overall fabric and evolution of states and human communities in the future.

The participants will be first asked to read individually this "vignette" and then to discuss the assumption about the future it includes. Then, the participants will have to discuss what other assumptions they have about the topic at hand and to collect them on a whiteboard. In order to have a focused discussion, each group will work on the particular topic on which they received the vignette.

The goal of this exercise is for the group to conduct a deliberative discussion about each participant's assumptions about the future. After each participant has presented his/her assumption, the group can discuss what they think about it: whether it is realistic or not, whether it is based on sufficient knowledge about the current development of Artificial Intelligence. At the end, each person's assumption is expected to have been improved by being subjected to the collegial scrutiny of others.

It is important at this stage to maintain a respectful approach and to criticize exclusively each other's visions.

Stage 3: Timeline – 30 minutes – Small groups of 5-8 individuals

At this stage, given that participants will have a more-or-less clear conception about how their imagined future will look like, they will be asked to position themselves at a moment in the near future (2025) and look into the past to draw a timeline on the whiteboard. On this timeline, they will place the relevant events that occurred in the field of artificial intelligence before 2021 or are likely to occur soon after, given the directions of current technological research.

Moderators will advise participants to use their mobile phones or the laptops provided in order to identify the relevant events, if they do not have already a clear view on which they are. At the end of the stage, ideas will be collected and participants will explain why they believe these ideas represent stepping stones to the future they imagine.

Stage 4: Policy recommendations – 30 minutes – Small Groups of five to eight individuals

At this stage, participants will be asked to think about what policies they would adopt in order to bring about the desired future/ avoid negative futures that they have imagined. They will be asked to think of themselves as a decision-maker / adviser to a decision maker that has the power to adopt a particular policy. The action has to be well justified and to address a concrete aspect which has the potential

to bring about/avoid the future imagined. In order to clarify the idea of relevant policy, the moderator can refer to three possible types:

- influencing people's behaviour or practices;
- influencing structures - legislation/taxes - which are coercively imposed by the state;
- influencing people's thinking – attempting to convince people to think in a particular way.

Each participant has to clearly explain the policy they would adopt and formulate concrete actions they would take.

The facilitator will encourage participants to avoid keeping things at a high level of generality and seek concrete solutions. Participants will be advised to be concrete about both actions and motivations. For example: "I would tax the use of AI-based gambling to a greater extent than regular gambling because the organizers have a higher chance of winning."

It will also be important to tie the recommendation to the future imagined in the first part. For example: "Through this, I will avoid the creation of gambling monopolies in the hands of those who use AI when organizing gambling."

> **NOTE:**
> At the end of the exercise, each group will elect a speaker who will present the group results in front of the whole assembly and the board of panellists. Each presentation will focus on the assumptions identified, timeline of events and policies to be adopted, as decided by the group.

Stage 5: Making assumptions about the future.

The following vignettes aim to illustrate the idea of assumption about the future. It presents a "glimpse from the future" which shows how a situation might develop based on a particular assumption which is not explicitly stated but can be inferred from reading the text. The goal of the exercise is to identify participants' assumptions about future trends and to challenge them through open discussion.

Vignette 1:
A glimpse from the future – politics and democracy

20.11.2050

Welcome to SELECTION DAY

Once again, dear viewers, we invite you to tune in for the next 15 minutes to be part of the wondrous moment that takes place every 5 years. Whether you choose to open your radios, TV or virtual reality device, it will still be irrelevant for who will our leaders over the next five years be.

However, we can still invite you to participate and to watch as ELECTOR 2.1™, the latest version of our leader-election artificial intelligence program will select all the five Members of Parliament and the Supreme Leader. Watching our program will, at least, give you the chance to imagine that 50 years ago you wasted much more time from your life for the task of selecting leaders. Imagine the waste: actually looking at the programs of each candidate and at their personal characteristics and then making a decision! I mean, really, ELECTOR 2.1™ integrates all this information a billionth time faster and can easily make the best decision within seconds. It quickly processes information about all people in our country such as reasonableness and level of patriotism and it chooses a Supreme Leader in seconds. Just think how politics was conducted 50 years ago. What was the point of having a two-chamber assembly? And a dedicated judicial branch? Leader's election process uses up so little time these days and reaches far better decisions! Just see the war we just won! And how quickly those guilty of sedition were dealt with, fractions of seconds after they were trying to assemble a "peaceful" protest against the war!

So, tune in minutes! Or don't! But be aware that ELECTOR 2.1™ will be working and a new leader will be announced 20 minutes from now. See you soon and all hail the new leader!

Vignette 2:
A glimpse from the future of AI regulated climate change mitigation and clean energy production

08.08.2050

Had we not acted in 2025 ...

Today, the International Committee for Climate Change Mitigation has reunited the world's climate change and pandemics mitigation policy makers and scientists in a global format, with the aim of evaluating of the progress made to curb the effects of global warming and related pandemics. One of the most invoked dramatic moments was that of the 2025 pandemic and climate change crisis that led to the signing of the Global Agreement and the setting up of the International Committee for Climate Change Mitigation.

"What if in 2025 we had not acted?", was the question addressed to the audience by the President of the Committee, who reminded participants that if drastic measures had not been taken in 2025, a significant part of the world states would have, by now, faced failure and massive migration, as well as calamities and death of the vulnerable population.

"Today, we can cope with the changes because 2025 stopped the world from a doomsday scenario minutes before the point of no return", she added, emphasizing "the importance of maintaining the rhythm of technological progress in mitigating climate change, as well as the need to step up the implementation of The Global Responsibility Act that allows the implementation of policy and climate security initiatives worldwide."

"The pandemic and climate change crises in the beginning of the 2020's had a major impact on humanity! A global change of mindset, advanced by scientists, shifted the focus of world economies from putting AI and robotics in service of increased industry efficiency to addressing the dramatic impact of climate change. First timid interventions and slow global change pioneered by the EU and the US has set the tone. Let us remember that 2025 was the year of massive worldwide popular protests, with not only the poor and third world

countries affected, but also the entire globe perceiving effects of draught and famine, severe floods and hurricanes. When another pandemic started from the deforested Amazon jungle, the Paris agreement and national policies proved their limitation and new drastic measures became necessary for humanity to survive. It was then that global leaders met, under the pressure of massive civic protests, and launched a global task force which was given responsibilities and power to enforce initiatives to mitigate effects and attempt to curb global warming. The world is still struggling today, in 2050, but survived the worst in the last 1000 years, with unprecedented mobilization and solidarity across continents.

And nothing would have been possible without AI and robotic technology now in service at global level! The sensors fly autonomously across the atmosphere and oceans to detect pollution, swarms of robots work in parallel to cover large areas and collect data about climate changes, robotic assistants are used to build and maintain across the world, regardless of national borders, renewable energy stations – from solar power systems, to wind towers, hydroelectric generating stations and the newly invented **Blue Tdor** technology that uses algae in the oceans to generate clean energy and power the agricultural and living domes that make our lives still possible!

Today, vertical agricultural stations in highly technologized domes enhance efficiency, reduce the use of chemicals and protect harvest from severe weather oscillations; Deepmind AI predicts well in advance wind patterns, which have become strong and rapidly changing. They help optimize wind farms and early warn citizens to start the shelter function in their collective AI managed homes. Recycling has become the norm and reduces the need to produce new resources, which are increasingly scarce. Robotic systems are also used to rescue the victims of the many temporary but also permanent floods that make people leave their homes behind due to the increase in the sea level. Fires have also become a regular challenge we get to be confronted with these days, and robots are used to rescue victims. AI is used to assists with post floods and post fire recovery and restoration of biological impacts, planting trees and regulating the number of invasive species that put at risk the frail ecosystem balance. None of

these circular, zero carbon footprint economy and lifestyle would have been possible for the world nations without the scientists' contribution to AI solutions to address climate change or the dramatic mobilization of world governments and policy makers! They saved the human race in the last hour of the planet. It is now up to us to build a future for the human race away from the point of no return that haunted our last 50 years!

Vignette 3:
A glimpse from the future of AI assisted medical system

27.05.2050

Meet MediChat – your medical personal assistant

Have you ever encountered any difficulties in making an appointment with your doctor or with a medical specialist to get treatment for a specific medical condition/problem? Xvitia comes now with the perfect solution for the struggle to visit a doctor!

Meet MediChat – your daily virtual assistant who brings the doctor into your house. You will be able to report to the Chabot your symptoms and health concerns at any time and the algorithms will diagnose your illness and will automatically schedule you to visit a specialist, either based on your preferences (introduced when creating your profile) or based on your location (the closest hospital to your home). MediChat has access to all the medical institutions, private and public, in your country and abroad, being able to offer you recommendations on the availability of specific interventions at medical institutions from other countries. When making the appointment, you can opt for a physical or online consultation, taking into account the seriousness of your illness and level of symptomatic discomfort, as well as the availability of the identified specialist. MediChat will also function as a reminder, sending you notifications when your appointment is due or when you should schedule your annual consultation.

The AI-app includes a feature of diagnose tracker that helps it to develop new medicine based on the symptoms claimed by all users. The collected data is sent to a system of super-computers that uses the information on biochemical ingredients in order to create and test new, targeted, adapted medicine, before sending the prescription to the MediChat.

The mobile app can be installed free of charge, being available on any operating system (IoS, Android etc.). In addition to the application, Xvitia has also launched the MediChat smart watch that automatically connects to the app and that collects data with regards to your medical condition, helping the app to permanently analyse your medical profile and identify any worrying changes that need further investigations. Imagine your phone will now be able to measure your temperature every morning and put you in contact with any specialist one click away! And when the time comes, it will be able to inform you that there are no more medical options available and that you can now schedule the termination program in the 3 months' timeframe indicated by the robot. Xvitia helps you take informed and timely decisions on your health and lifespan!

Vignette 4:
A glimpse from the future of AI for autonomous or self-driving vehicles

20.11.2050

Meet the next-generation #Robotaxi

Dear father,

I sent you a hologram message from 2050 Phoenix, where 30 years ago we used for the first time a Robotaxi. Do you remember when we were included in the first fully self-driving taxi service developed by Google, Waymo One, legally allowed to operate in Phoenix, Arizona USA, in May 2021?

It was just the beginning… and at that moment we could not imagine the evolution of the transportation market with the complete

expansion of Artificial Intelligence in the development of fully autonomous vehicles. If 30 years ago, the AI technology research was focused on traffic and navigation system, today, the company that I am working for shifted focus to make fully autonomous cars integrating the custom-built and high-performance computer solutions.

The complexity in software also increased exponentially, with an array of redundant and diverse deep neural networks (DNNs) running simultaneously as part of an integrated software stack. Huge sums were invested by both technology companies and traditional car-makers, from Waymo One, Zoox, Voyage in the U.S., to DiDi Chuxing in China, to Yandex in Russia.

Imagine that people in every part of the world are able to order a driverless Robotaxi and use it for weekly shopping, nights out and without challenges as leaving the motorway or roads closed off with traffic cones, difficulties that we encountered with Vimeo One in 2021.

Now we can request a fully autonomous vehicle through the ROBOTAXI GO app. The app includes virtual reality navigation while the vehicle features remote car honking, allowing users to easily locate it. To unlock the vehicle we simply scan a QR code with health information for pandemics prevention purposes. Than we give a simple 'Start the Journey' voice command. The vehicles do not have safety drivers behind the wheel, but they do feature a 50G-enabled remote driving service that allows a Robo-remote operator to control them in the event of an emergency.

Each ride costs only 4 MercurCoins, and the service is open to passengers aged 18 to 100. So you are invited to use frequently the next generation #Robotaxi, a complex supercomputer on wheels. The car is fitted out with high-definition cameras and sensors that collect data and feed it into a machine-learning application. Moreover, the autonomous vehicles are constantly upgradeable to take advantage of the latest advances in AI algorithms, the language of the future, as you predicted when I was a child.

Yes, you are right… Seniors need a safe and affordable Robotaxi service. That is why, with the next generation of #Robotaxi all concerns towards safety and security completely disappear! Only one small thing has delayed the launch on the market – and that is the NGOs that keep

protesting on ethical issues and refuse to understand that all progress comes with risk. So what if some individuals have died due to AI decisions in inevitable car accidents? AI has calculated which route variant implied a lesser number of victims, and that should be enough!

However, the demand and adoption of AI technology in transportation are increasingly growing and we are ready to see drastic changes in the domain every year!

So, dear father are you ready to meet the next-generation of #Robotaxi?

Love, Peter!

Vignette 5:
A glimpse from the future of AI for teaching and education

21.09.2050

International teacher's conference 2050

Today's panel featured a discussion on the best teaching methods to be applied with teenagers and university students. Three participants took place and each had the opportunity to share some of their experiences featuring the education of the relevant age group. Especially, during the age of virtual reality, which can confuse some of the very young minds, it is crucial to develop critical thinking and the ability to distinguish between virtual and real realities.

TEACHER 1.0, created by IntellTech Corporation, showed how it exposes high-school and university students to virtual reality in a controlled environment and how it shows them that in virtual reality certain physical laws can be broken, which would not be possible in the real world. This is exemplified by the fact that in virtual reality, animals, such as pigs, can be programmed to fly, which, attempted in the real world, would be prone to fail.

ACADEMOR, programmed by the Research and Academic Writing Laboratory of the Department of Homeland Security, showed the latest trends in security studies paper writing and how this can be done in virtual reality. However, it highlighted the fact that papers

written in virtual reality might not be accepted in proper conferences, as they rely on empirical results which are not possible in the real world. It exemplified this with a paper describing the results of a battle simulation where one tank was able to destroy more than 50 others without sustaining any damage. Later, it was found that the programmers of the virtual reality had cheated and made that tank invulnerable.

SPORTSMAN 3.5, funded by Grime Corporation, focused on the effects of virtual reality on sports education and illustrated its presentation with real-life injuries of young people who attempted the same basketball schemes in real life as those in virtual reality.

At the end, the three participants concluded that a stronger approach is needed to clearly explain to students that virtual reality can be programmed based on laws of physics different than those of real life, but that addiction to virtual reality can lead to severe physical and psychological damage.

What assumption about the future is illustrated in the text? What other assumptions about the impact of Artificial Intelligence on education do you have? Discuss with your peers.

PRACTITIONERS' BROAD VIEW

THE DARK WEB – A USEFUL TOOL FOR THE OPEN SOURCE INTELLIGENCE GATHERING (OSINT) AND A CHALLENGE FOR THE SECURITY SECTOR

GIS Representative*

Abstract:

The spread of the global network (the Internet) throughout the public has completely changed and simplified the means of communication, exchanging information and the working process. It has become a useful tool for specialists represented in almost all fields, as it allows them to quickly search, verify and share information. The Internet has greatly simplified and increased the effectiveness of the working process of the Government Agencies, including those that are represented in the security sector. Nevertheless, it also created new challenges which can pose a threat to ordinary citizens, different groups, organizations and Governments. Countries were forced to adapt and integrate new ways of working in order to prevent and counteract novel security threats. Some divisions represented in the security sector had to completely transform in order to combat new challenges.

Due to the fact that the law enforcement agencies are able to fight cybercrime in the "Surface Network", the "criminal world" of the Internet has shifted to a completely different Internet space – The Dark Web, where it tries to bypass the law without leaving any trace by using a variety of available software, thus creating a serious threat for the Global Community.

Keywords: *global network, dark web, security, OSINT.*

Introduction

Kaspersky Lab blog state that "the Internet is sizable with millions of web pages, databases, and servers all running 24 hours a day. But the so-called "visible" Internet (aka *surface web* or *open web*) that most of us use on a daily basis and can be found using search

* Georgian Intelligence Service (GIS).

engines like Google and Yahoo – makes up under 5% of the total internet and is considered to be only the 'tip of the iceberg'." As for the Internet that is unreachable (or reachable through special software) for ordinary citizens, also known as "Deep Web" and "Dark Web", it accounts for up to 95% of the whole Internet Space (Kaspersky Lab blog; McAfee blog; Norton blog). Most people often use the term "Deep Web" when talking about the "Dark Web", but they both differ in nature.

"The Deep Web is part of the World Wide Web whose contents are not indexed by standard web search-engines (e.g. Google, Yandex, and Bing) and makes it hard for the law enforcement agencies and ordinary people to search for the specific websites." (Karpersky Lab blog) The opposite term is "surface web", which is readily available to the general public and searchable with standard web search engines.

The Dark web refers to sites that are not indexed and can only be accessed via specialized software (e.g. TOR, I2P, and Freenet). Significantly smaller than the tiny surface web, the dark web is considered a part of the deep web. The specialized software helps the Internet user to access the unreachable web by hiding his/her IP address, thus ensuring anonymity.

"Even if the cover of the dark web often keeps law enforcement at bay, basic tools can enable anyone to engage dark web services without much difficulty. Basic internet literacy, a computer, and access to the internet are enough for any sufficiently motivated individual to begin supplying or purchasing illicit goods on the Dark Web." (Karpersky Lab blog)

The Deep Web

The deep web accounts for approximately 90% of all websites and is considered to be "much larger than the surface web. In fact, this hidden web is so large that it is impossible to discover exactly how many pages or websites are active at any one time." (McAfee blog) According to some sources, the Deep Web holds approximately 7.5 petabytes – about 400-500 times bigger than the Surface web. As already mentioned, the content of the Deep Web is not indexed by standard web search-engines, which makes it hard for internet users to directly access its contents. "While many news outlets use 'deep web'

and 'dark web' in the same context, in fact, Dark Web is the part of the Deep Web, which is mostly legal and safe. Some of the largest parts of the deep web include":

- "Databases: both publicly and privately protected file collections that are not connected to other areas of the web, only to be searched within the database itself."
- "Intranets: internal networks for enterprises, governments, educational facilities and groups of individuals used to communicate privately and control aspects within their organizations."
    - The user should know the direct link of the non-indexed website he/she wants to access. However, the given resource may require the visitor to enter a password, which must either be created during registration, or received directly from the owner or a member of the website.
    - Access to the content is decided by the Admin, who sets the list of IP addresses of computer users with access to the website.

Some of the Deep web sites "may be concealed behind passwords or other security walls, while others simply tell search engines to not "crawl" them." Without visible links, these pages are more hidden for various reasons. Their "hidden" content is generally cleaner and safer. Everything from blog posts in-review and pending web page redesigns, to the pages you access when you bank online.

Dark Web

Like the "Deep Web", the Dark Web's content is also not indexed by standard web search-engines and, in order to access it, the Internet users must install special software, such as TOR, I2P, and Freenet, which also ensures their anonymity. "Dark Web can be small peer-to-peer or friend-to-friend networks, as well as large networks like Tor and I2P operated by organizations and individuals. The Tor network focuses on providing anonymous access to the Internet and I2P specializes in anonymous hosting of websites." (Karpersky Lab blog)

It is possible to identify the owners of non-indexed websites located in the Deep Web with the help of different technical means (e.g. it is possible to determine who buys, who visits and to whom the website domain is registered), but this is impossible in the case of the "Dark Web", due to the fact that it was created by using the TOR / I2p / Freenet network. The Dark Web websites do not share the same principles of naming their domain like the Surface websites (e.g. bbc.com, facebook.com, google.com). The Dark Web domain consists of various characters (numbers, letters, etc.) and ends with .onion or .i2p (similar to the surface web: .com, .ru, .com.uk). It is not possible to access websites ending in .onion or .i2p through normal browsers as they are not part of the DNS system. Onion websites are only perceived by Onion servers.

As already mentioned, the software used to access the Dark Web allows users to surf the Internet anonymously by avoiding the Government institutions and without leaving traces. This creates a ground for journalists, bloggers, various opposition groups, or followers of certain ideologies to use the Dark Web as a platform to exchange information, discuss various issues and express their opinions freely. Likewise, free e-libraries and banned literature are also available for the web users. However, the Dark Web is actively used by individuals who are involved in criminal activities.

The Dark Web is mostly used for drug trafficking and there are many websites that offer users a vast variety of drugs. The most well-known website that was used as a platform to sell drugs and other illegal products was – The Silk Road (known as the Amazon.com of the Dark Web). The Website was shut down by the US Federal Bureau of Investigation in 2013, but it didn't solve the problem; if anything, it made it even worse as it led to the creation of many other websites with similar content.

Buying drugs is not the main interest for most Dark Web users. "Customers" have access to the illegal trade of classified information and weaponry. They can also view/order sadistic videos and child pornography in exchange for crypto currency, purchase personal information about individuals (passwords to various accounts, information on bank debit cards etc.), organize a terror attack, hire

hackers and hitmen for various tasks and order fake documents. The users carry out the aforementioned illegal activities through various websites, forums, online stores and social networks. There are speculations that there are websites related to the so-called "Islamic State", through which young people around the world are recruited and become part of organized terrorist attacks.

The Dark Web can be used by certain groups driven by anti-state interests and might be directly/indirectly controlled by other states; if necessary, other states can also aid the members of the covert group with financial support (with crypto currencies) and, if needed, provide them with an action plan and advice. The Dark Web might also be used as a communication platform by opposition forces against the government (e.g. the opposition Tor during the Arab spring)

The law enforcement agencies throughout the world are actively involved in the Dark Web (also Global Web) monitoring process in order to: identify individuals involved in criminal activities; detect a leak of classified/personal information and take measures to delete it; identify dissident groups working for other states.

Although detecting threats in the Web might seem complicated, law enforcement agencies are still able to successfully identify illegal activities through the joint efforts of OSINT, SIGINT and HUMINT units (Easttom, 2018; Froomkin, 2015, Kumar and Rosenbach, 2019).

Dark web as a source for OSINT gathering

"Open Source Intelligence (OSINT) gathering and a proper understanding of the Dark Web are the first step in combating the Internet's dark spaces. With an understanding of how to use open source encrypted anonymity services safely, organizations can explore OSINT sources – which include web-based communities, user-generated content, social-networking sites, wikis, blogs and news sources – to investigate potential threats or analyse relevant information for business purposes." (McAfee blog) As already mentioned, the Dark Web has become a platform for journalists, anti-state-minded citizens, dissidents and public officials with harmful intentions to share/leak various types of information. Web users will often come across classified documents belonging to private companies

and Governments, which were obtained as a result of cyber-attacks carried out by hackers on the servers of the aforementioned institutions. It should be noted that there have been many cases of leaked classified information which negatively impacted some states and defiled their reputation. Searching for the leaked documents is considered to be one of the main interests of OSINT gathering and many of the obtained papers are valuable for their contents.

Cases of leaked information on the Dark Web

Databases of the agencies of different countries containing information about citizens have been repeatedly leaked into the Dark Web.

WikiLeaks. A website that publishes classified documents provided by anonymous sources and hackers. The information posted on the website has not once received international attention and even caused diplomatic scandal. Access to WikiLeaks is also possible with ordinary browsers (Chrome, Opera, Firefox), although most of the documents posted on the website are available only on the Dark Web version of WikiLeaks

In 2019, hackers leaked data on 267 million users of the social network Facebook, which contained information about their identities, dates of birth, addresses and Facebook IDs. The leak mainly affected the Facebook users living in the US;

In 2019, hackers obtained information on nearly 620 million users registered on 16 popular websites which, in addition to identities and other personal data, contained user accounts, passwords and Debit Card information.

In 2020, information on 500,000 users (including accounts and passwords) of the video-telephony software program ZOOM was made available on the Dark Web. Information on most of the accounts was for sale (approx. 1 US cent per account) but some pieces were provided for free.

Examples of Dark Web websites that can be used for OSINT gathering

The information and websites on the Dark Web can be accessed through search engines designed specifically for the web, although most websites require the knowledge of their direct links. There are many websites that provide a long list of various websites, although the data may be obsolete because the websites on the Internet are not stable - they are often deleted by various law enforcement agencies (if the website is illegal), or by the owners themselves. There are many sources that are considered interesting for OSINT gathering, including some of the websites given below:

Tor Facebook (facebookcorewwwi.onion)

- Facebook created a special address for users to access its website securely with an end-to-end encryption. Ideally, this means that Tor users, some of whom may be using the software to circumvent government censorship or restrictions of the internet in places such as China or Iran, will be able to use Facebook reliably and without worrying about leaking their personal information. It is reported, that TOR Facebook is being used by over 1 million people monthly.

The Hub

- It is considered to be the largest discussion forum on the dark web focused on dark net market, reviews, crypto currency and cyber security. The forum gives its users access to a variety of groups of interest. According to the recommendations provided by Internet users, in order to get acquainted with the Dark Web, you must join The Hub.

Sci-Hub

- A large database of scientific papers from around the world that was obtained and uploaded by hackers. Anyone can read and download papers prepared by scientific institutes.

ProPublica

- An investigative journalism outlet which has a presence on the surface web but also a dark web link. This way, visitors of the website can remain anonymous if they want to. This could come in handy for people living under oppressive

regimes, for instance. After all, ProPublica doesn't shy away from covering controversial topics, such as child labour and corrupt politicians. ProPublica publishes news stories in both English and Spanish.

SecureDrop

- A place where whistle-blowers and journalists meet. The dark web is one of the only ways for whistle-blowers to share their information while being certain they won't be tracked down. Whistle-blowers often have damaging information about a company or government and try to share this with journalists. If they do so, on the surface web, they'll likely be traced and, in some cases, punished. SecureDrop is an .onion website that protects the privacy of whistle-blowers and journalists all over the world. Many important publishers and news organizations have realized the power of anonymous whistle-blowers on the dark web and have set up their own SecureDrop URL. Some notable examples include: Forbes: http://t5pv5o4t6jyjilp6.onion/; The Financial Times: http://xdm7flvwt3uvsrrd.onion/; and Reuters: http:// smb7p276iht3i2fj.onion/

Conclusions

As already mentioned, the use of illicit Internet is on the rise and the Dark Web has become a platform for criminal activity, where users roam freely and get involved into various illegal deeds. Although law enforcement agencies have witnessed a steady expansion of dark web activities, they largely lack quantitative data to inform effective responses and solutions to dark web activities.

The Dark web activity crosses national borders. The cross-jurisdictional nature of the dark web makes it essential that investigators collaborate across agencies. Therefore, the law enforcement agencies of various countries must cooperate in order to counter the incoming threats more effectively and in time. Constant communication, sharing information and personal experiences between the partner organizations will play a vital role in this regard.

Specialists states that: "The 'dark web' is an internet shadow world where the good and the bad co-exist. On the good side, the dark web provides anonymous, secure communication channels to shield classified government activity and protect reform agents such as human rights activists and journalists opposed by oppressive foreign regimes. On the bad side, the dark web has emerged as an important hub of criminal commerce, a fully functional marketplace where hidden customers can buy from hidden sellers with relative confidence, often with customer ratings available, just as on the public-facing web."

References:

1. Easttom, Chuck, (2018). "Conducting Investigations on the Dark Web", *Journal of Information Warfare*, vol. 17, Issue 4. Available on https://www.jinfowar.com/journal/volume-17-issue-4/conducting-investigations-dark-web

2. Froomkin, Dan. (September 11, 2015). *FBI Director Claims Tor and the "Dark Web" won't let criminals hide from his agents.* Available on https://theintercept.com/2015/09/10/comey-asserts-tors-dark-web-longer-dark-fbi/

3. Kaspersky Lab Blog. (n.d.). *What is the Deep and Dark Web?*, Available on https://www.kaspersky.com/resource-center/threats/deep-web

4. Kumar, Aditi, Rosenbach, Eric. (September 2019). "*The Truth about the Dark Web.* Intended to protect dissidents, it has also cloaked illegal activity", *Finance & Development*, International Monetary Fund, Vol. 56, No. 3. Available on https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf

5. McAfee Blog. (August 24, 2015). *The Mysterious, Ominous Dark Web: A Primer for the Rest of Us.* Available on https://www.mcafee.com/blogs/internet-security/what-the-dark-web-is/

6. Norton Blog (n.d.). *The emerging threats. What is the dark web?* Available on https://uk.norton.com/internetsecurity-emerging-threats-what-is-the-dark-web.html

7. Leigh, David, Harding, Luke. (2011). *WikiLeaks: Inside Julian Assange's War on Secrecy*, London: Guardian Books.

8. Tor Project website. Sponsors. Available on https://www.torproject.org/about/sponsors/

REVIEWS AND NOTES

Dorin Mihai RÂNCEANU, *ROMANIA*
***PART OF THE EUROPEAN RISK ECOSYSTEM*,**
Tritonic Publishing House, Bucharest, 2018, 156 p.

Review by Ionuț HOREANU

Romania part of the European risk ecosystem is a book which managed to extract from a seemingly sterile subject – perhaps with implications strictly related to the sphere of some professionals – an analysis with the true value of a study, by treating in a concise, clear and coherent way a topic proven to be important precisely through the form and content of the research. The book is structured into seven parts: *Introduction, The need to define the concept of security in the current dynamics of international relations, Actions that changed Romania's geopolitics, Use of risk ecosystem in hybrid aggression, Specific threats to the European risk ecosystem, Vulnerabilities specific to the risk ecosystem European and the last section of the conclusions*.

Its aims is to detect the geopolitical issues of the Romanian state, from the geopolitical position of Romania, determined by the military, strategic, economic and ideological dimensions, and to explore the defining elements for geostrategic directions. The author, Dorin Mihai Rânceanu, analyses Romania precisely through the valences of the risk ecosystem. He considers that our country makes a significant contribution to regional and global contingency reporting, articulating the meaning of "interconnecting threats and vulnerabilities in a European risk ecosystem" (p. 9).

Right from the onset of the analysis, after the introductory section, the researcher articulates the thread he will try to follow in the paper, as well as the stake: "interconnection and complementarity of asymmetric threats and vulnerabilities", which lead to shaping a "risk ecosystem used by Russia in order to change the balance of power in the eastern part of the NATO/ EU flank" (p. 11). In the second section of the book, the mechanisms of the involvement and influence of the Russian Federation is analysed through the three theoretical perspectives of the international environment: realism, liberalism and constructivism. On this occasion, the author points out that Russia's concern is to ensure the image of a state that does not compromise the principles of international liberalism (p. 13). The pages devoted to the study of liberalism as a means for understanding the „need for security through cooperation" have the role of highlighting one of the positions that Romania must adopt, with the reasons derived from current liberalism (p. 16). Therefore, the author shows that unlike structural realism, liberalism supports the growth of both absolute and relative power. It is important to highlight that the study guarantees the limits of introduction in security and geopolitics. The analysis of constructivism is necessary for the exposure of security mechanisms because the relationship between collective cultural values and the direction of the state at the international level is not excluded. In this way, regional alliances within NATO or the EU can be explained.

In the third section of the paper, *Actions that changed Romania's geopolitics*, the influence caused by Russia's position through the "hybrid scenario of taking power over neighbouring states" is analysed (p. 25). In the context of Romanian geopolitics, at the intersection with Russian geopolitics, this section emphasizes the impact that the Romanian state could experience in the case of relations between a neighbouring state and the power in Moscow, if a security risk should

arise. For this reason, the author extensively explores Russia's links with: a) Ukraine – where he observes a double dependence on the EU and Russia, and the role shown to Romania is to counter military, separatist, extremist threats, etc., through proactive actions; b) Moldova, where the author highlights the different situation of Chișinău, which is inclined towards the West, and Tiraspol, inclined towards the East; c) Serbia, a state which does not belong to NATO or the EU, and the steps towards European integration are made with the help of Moscow, an important role being played by the support of Russian gas projects, non-recognition of Kosovo, etc.

Another dimension of the research touches on Russia's relationship with Romania's NATO neighbours: a) Bulgaria, highlighting the dependence on Russian gas (90%), the interests of the Russian oligarchy, the interference in the administration of cross-border organized crime, the Bulgarian Russophile sentiment and the use of the Bulgarians as a Trojan horse in NATO decisions; b) Hungary, highlighting the propaganda messages of social radicalization (xenophobic orientations of far-right parties in connection with Romania and Ukraine). The influence of the events in MENA (*Middle East and North Africa*) on the geopolitics of Romania is also discussed. Attention is drawn to Europeans radicalized on the Internet and connections with terrorist groups, but also to the "Balkan route", because it can lead to an increase in the number of refugees in Romania, in the MENA region (p. 46).

The fourth section of the book discusses the use of the risk ecosystem in hybrid aggression (terrorism, immigration, piracy, corruption, ethnic conflict etc.), which comes with new strategies, instead of the classic armed struggle. Against this backdrop, the involvement of the aggressor state is difficult to prove. A part of the hybrid threats can be transnational networks, from criminal groups in

the drug and weapons sector, financial activities, involvement through facilitators (media companies, terrorist NGOs, corruption of dignitaries, military aggression etc.) (p. 52). Likewise, facilitators can play an important role in the exploitation of decisions with legislative impact, involvement in and through multinationals, etc.

The next section of the book examines how Russia acts to increase influence and, implicitly, power, through hybrid warfare. On the one hand, asymmetric threats (cross-border organized crime, cyber-crime, economic crime, espionage, terrorism etc.) are analysed by facilitators, and on the other hand, unseen directions and levers for the vulnerability of states and cooperation systems are brought to attention (p. 56). These boundaries show how crime networks have been transformed into "interstate structures similar to global, corporate or multinational concerns" for "organizational flexibility and action efficiency, making it difficult to identify leaders" (p. 62).

The author also analyses another phenomenon produced after the disintegration of the USSR, when a network of former KGB officers, through facilitators from European countries (lawyers, accountants, bankers with offshore accounts from around the world) laundered money abroad and returned to take power: "these facilitators have created for the Russian Federation a real network that currently has a hidden power at European and global level" (p. 63). Regarding Russian oligarchs, the author believes that they can be identified as members of an organized crime network – Russian intelligence officer (under commercial cover, especially energy), representative of a Russian company – all three qualities in one person, but also none. This question further articulates the size and proportions of crime forms (p. 69).

The next of analysis is the terrorism (p. 75), analysed from three perspectives: a) anarchist; b) secessionist; c) anti-colonial and nationalist. Multiculturalism or migration can be placed in the same

register. An extension of these can be found in religious terrorism, considering that such groups "transcend national loyalties" by joining volunteers with poor psycho-social training from third countries. This idea is supported by the voice of sociologists (Durkheim) who consider suicide as "the result of poor integration" (p. 87).

An important subsection is the one regarding the threats to energy security. The author analyses the hybrid vulnerabilities of Bulgaria and Hungary, which can have repercussions on Romania as well. Thus, the "roads of Russian energy" to Austria pass through Serbia and Hungary, and the one to the Italians "feeds" the Bulgarians and Greeks. In light of these directions, the "red lines" of the Russia Federation were drawn, so that they separate the European states into pro and anti-Moscow (p. 91). Romania's strategic partners, Hungary and Bulgaria, have supported Russian interests by setting up joint ventures with Gazprom, noting that national interests may be at odds with those set at European level. The author state that Romania's relationship with the Caucasus states may reduce energy threats. Eloquent is the Nabucco project which involves the transport of gas from Azerbaijan through Georgia or Iran, to Turkey, Bulgaria, Romania, Hungary, and Austria.

The penultimate section addresses the vulnerabilities specific to the European risk ecosystem:

a) vulnerability through the use of elements of strategic communication and information warfare, bringing to attention issues regarding:

- psychosocial representation of security – social identities and common values can be vectors of power influenced by soft power, propaganda, information warfare, starting from messages with the myths of war, the dictatorial image of leaders etc.;

- soft-power as a method of vulnerability and radicalization of Europeans - imposing the will on some groups through political, cultural values etc.;
- information war - divided into war of command and control (cancellation of decision-making capacity through psychological mechanisms, due to misinformation, manipulation of information on which the decision should be taken);
- psychological warfare – aims to change attitudes, behaviours, perceptions;
- economic information war – information war related to the economic war.

b) Vulnerability through the use of asymmetric threats in subversive attacks is possible through the following forms:

- racism and xenophobia as a threat to national security;
- hooliganism – a form of extremism and separatism, based on stereotypes, prejudices (e.g. feeling of Islamophobia);
- Euroscepticism and political extremism – forms of diminishing international cooperation – populist parties, promoting the superiority of race, ethnicity, religion etc.

A special role in the information war is identified in the direction of the Romanian Orthodox Church (BOR) and NGOs. Putin considers Russia "the guardian of Christianity". Even the European Parliament recognizes the role of the BOR in the „offensive strategic communication of the Russian Federation" (p. 125).

c) Vulnerability through the exploitation of legislative gaps: lawfare, in connection with the information war has the role of abusive use, circumventing or undermining certain legal provisions, claiming to be defenders of certain areas or populations, at the limit of international provisions.

In the geopolitical analysis of Romania, we notice that the international theories and principles also have an echo on the eastern space, where the stake is represented by the increase of the relative power, together with the weakening of other states. The solution required after the analysis of the book is that Romania must relate to risks according to its own security interests. In conclusion, it becomes obvious that we have reviewed a work without *parti pris*, a study difficult to perform, taking into account the objective achieved. The author uses a topicality of ideas and events, and through the connections between them he manages to achieve his proposed goal, to reveal the geopolitical situation of Romania as part of the European ecosystem of risks.

ACADEMIC FOCUS

Education, Scholarships, Apprenticeships and Youth Entrepreneurship Programme in Romania, funded by the EEA Grants – Financial Mechanism 2014-2021
Agreement no.: 18-COP-0017
(October 1st, 2019 – March 31st, 2022)

THESEUS Project aims at Connecting the Disconnections between Disparate Data, in order to provide knowledge for building Insightful Analysis. The broad availability of data has led to increasing interest in methods for extracting useful information and knowledge from data, determining the emergence of new fields of science (e.g. data science). At the same time, big data algorithms have been signaled as a potential leverage that can lead to digital dictatorship if insufficiently understood, poorly handled and unethically regulated. Companies in every industry focused on ways to structure, process and analyze the growing volume and diversity of data so as to streamline decisions and gain a competitive edge. State institutions, regular citizens, social and political science practitioners on the other hand, are not yet properly equipped to properly mitigate the economic, social and political impact of the information technology revolution that awaits us in the decades to come. Therefore, in the process of understanding and mitigating risks and opportunities of Big Data, complex workloads, new skills and competences have to be acquired.

Following these emerging needs, the **objective of the project** is to enhance human capital and knowledge base by tackling directly skills and competences required and providing an understanding of the

processes guiding big data analytics. This objective will be met by **building and delivering a course**, consisting of four modules, capitalizing on big data methodologies: introductory module, data collection module, data processing module and data analysis module.

The course will not be designed as a technologically focused course, but rather knowledge, awareness and understanding focused course. The course avoids an algorithm-centered approach. It focuses on how options are understood and choices and tradeoffs are designed. Thus, it enhances, through learning by doing, key-competences and skills required in collecting, understanding, correlating and processing big data, helping them streamline problem-solving processes in a data-driven ecosystem.

The project addresses **two professional categories:** *governance and social scientists* and *national security practitioners*, whose complementary work is of paramount importance in insuring the sustainable development of democracy. Both categories carry out great responsibility at social level. Ill-informed decisional processes in national security and policy-making, based on incomplete, inaccurate or incorrectly correlated data generate negative impact, affecting society at large. Although practitioners targeted by the project work with large amounts of data, their background is mostly in social science or security studies, lacking a very specific technical training. Such (future) professionals need to better understand what and how big data can be capitalized so as to ethically and lawfully improve the overall efficiency of their organization.

Participating organisations are: "Mihai Viteazul" National Information Academy (ANIMV) – Romania; University of Malta (UoM) – Malta; Norwegian University of Science and Technology (NTNU) – Norway; National University of Political Studies and Public Administration (SNSPA) – Romania. THESEUS Project is part of the Education, Scholarships, Apprenticeships and Youth Entrepreneurship Programme in Romania, being funded by the EEA Grants – Financial Mechanism 2014-2021.

Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
H2020 Grant agreement no: 883054
(May 2020 – April 2025)

EU-HYBNET is a 60 month project (2020-2025), financed through the Horizon 2020, which will start in May 2020. The project is being developed and implemented by a consortium of 25 partners, coordinated by LAUREA University of Applied Sciences from Finland. The European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre are leading partners of the EU-HYBNET project.

EU-HYBNET will bring together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats, by undertaking an in-depth analysis of gaps and needs and prioritizing those that are crucial to address through effective research and innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which will lead to the creation of a roadmap for success and solid recommendations for uptake, industrialization and standardization across the European Union.

The project aims to build an empowered, sustainable network, which will:

- define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavors;
- monitor significant developments in research and innovation;
- deliver recommendations for uptake and industrialization of the most promising innovations that address the needs of

practitioners, and determine associated priorities for standardization;
- establish conditions for enhanced interaction among its members;
- persistently strive to increase its membership and continually build network capacity through knowledge exchange.

EU-HYBNET will address four core themes to ensure coherence in the project's results: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration and 4) Information and Strategic Communication.

Romania represents the consortium through "Mihai Viteazul" National Intelligence Academy (MVNIA). MVNIA will incorporate the project's research findings and information into its MA & PhD research programs. As students come from diverse areas (security practitioners, legal, media, private business), the impact of exploitation of the information will reach a wide audience, and the EU-HYBNET training documents will also be employed to enhance capabilities of experts and practitioners in the fight against hybrid threats.

EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academia, industry players, and SME actors across EU, collaborating with each other to counter hybrid threats.

With the support of the Erasmus+ Programme of the European Union

Jean Monnet Module
EUSEGOV (2020-2023)
621227-EPP-1-2020-1-RO-EPPJMO-MODULE

Jean Monnet Module EUSEGOV

A common understanding of EU Security Governance
Teaching and researching the EU security policies and institutions for a better academic and professional approach in the security and intelligence field
(October 21st, 2020 – October 20th, 2023)*

"Mihai Viteazul" National Intelligence Academy (MVNIA) implements a three year Jean Monnet Module grant: **EUSEGOV** – *A common understanding of EU Security Governance. Teaching and researching the EU security policies and institutions for a better academic and professional approach in the security and intelligence field*. The EUSEGOV module focuses on EU Governance, a subfield of EU studies that has received less attention comparatively with the study of other EU related issues. The module aims at educating students and at equipping them with the knowledge and necessary skills to become EU citizens and better security providers. The academic value of the EUSEGOV module is to deliver courses on EU Security Governance for security and intelligence studies students. The courses tackle specific aspects of EU integration studies: *Introduction to EU Security Governance and Strategic communication in EU Security Governance.*

* This Project has been carried out with the support of the Erasmus+ programme of the European Union. The content of this Project does not necessarily reflect the position of the European Union, nor does it involve any responsibility on the part of the European Union.

The **specific objectives** of the Module are:

- Providing a coordinated series of MA compulsory and PhD summer courses aiming to familiarize students with the main trends and approaches in the field of communication and security governance in the European Union.
- Updating the teaching contents on the topic by research activities.
- Making aware students who do not automatically come into contact with EU studies of the importance of security governance by training them in using both the specialized language and methodology specific to subjects that pertain to the area of international relations, political sciences, as well as security studies.

The module's objectives will be achieved through the **teaching, researching and promoting** activities. To this respect, the EUSEGOV module includes a **two completely new courses**, one compulsory for MA students and one optional for PhD students, covering a major gap in the curricula i.e. the developments in the idea of European Security Governance. By bringing together academics and experts from various fields of knowledge, from civil society organizations and institutions, the interdisciplinary teaching and research approach of this Module provides the students with an in-depth and systematic understanding of key EU Security Governance topic. The EUSEGOV includes also research activities on the **Strategic communication in EU Security Governance thematic**. The research report will contain an extensive analysis of three aspects: *Strategic communication in EU – practices and official documents*; *EU Security strategic communication institutions*; *EU Security Governance future: alternative scenarios*.

A general dissemination campaign will be implemented to create a broad understanding of the importance and the particularities of EU Security Governance: two conferences, opening and closing conferences; a MA and a PhD round-table debates The main output is represented by the training of a target group formed by master students and PhD candidates in security and intelligence studies that must better understand the direct and indirect implications of EU's security governance impact on the member states.

CALL FOR PAPERS *ROMANIAN INTELLIGENCE STUDIES REVIEW*

"Mihai Viteazul" National Intelligence Academy, via its National Institute for Intelligence Studies, publishes the *Romanian Intelligence Studies Review* (RISR), a high quality peer reviewed and indexed research journal, edited in English and Romanian twice a year.

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Intelligence in the 21st century
- Intelligence Analysis
- Cyber Intelligence
- Open Source Intelligence (OSINT)
- History and memory in Intelligence
- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. The

editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or rejects notification being transmitted via email within 5 weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 27 and 28 and which is scheduled to be published on June and December, 2022.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and http://www.animv.ro for author guidelines. For more details please access the official website: **rrsi.ro**

Contact: Authors interested in publishing their paper in RISR are kindly invited to submit their **proposals electronically in .doc/.docx format at our e-mail address rrsi@sri.ro, with the subject title: article proposal.**

Appearing twice a year, the review aims to place debates in intelligence in an institutional framework and thus facilitating a common understanding and approach of the intelligence field at national level.

The target audience ranges from students to professionals, from the general public to those directly involved in intelligence research and practice.

ISSN - 2393-1450
ISSN-L - 2393-1450
e-ISSN 2783-9826

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

National Institute for Intelligence Studies

20, Odăi Str.
Bucharest 1 - ROMANIA
Tel: 00 4037 772 1140
Fax: 00 4037 772 1125
e-mail: rrsi@sri.ro

www.animv.ro