ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 1(31)/2024

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 following international databases: ROAD, CEEOL, EBSCO, DRJI, DOAJ, ASCI, SUDOC, HEINONLINE.

Bucharest
2024

CONTENT

INTELLIGENCE AND SECURITY IN THE 21ST CENTURY 5

Domenico FRASCÀ, Giulia VENTURI, Maria USTENKO, Alessandro ZANASI, Andrew STANIFORTH, David FORTUNE,
THE ROLE OF HUMAN INTELLIGENCE IN THE AGE OF DIGITAL TECHNOLOGY 6

Sanja TEPAVCEVIC,
(COUNTER)BALANCING THE WEST: RUSSIA'S INFLUENCE IN THE WESTERN BALKANS SINCE THE END OF COLD WAR 25

OPEN SOURCE INTELLIGENCE 51

Ainara BORDES PEREZ
WHAT IS REALLY "OPEN SOURCE INTELLIGENCE"? A CONCEPTUAL ANALYSIS OF THE DIFFERENT NOTIONS OF OSINT 52

CYBERSECURITY 75

Dragoș VETRESCU
BETWEEN GLOBAL VULNERABILITIES AND REGIONAL REALITIES: CYBERSECURITY DYNAMICS IN EASTERN EUROPE 76

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY 103

Anastasios-Nikolaos KANELLOPOULOS,
THE HAWALA SYSTEM IN THE WESTERN BALKANS: CHALLENGES AND STRATEGIES FOR COUNTERTERRORISM AND COUNTERINTELLIGENCE 104

Alina-Bianca COSCA,
LIVE TERROR A NEW WAY/MODEL OF ONLINE RADICALIZATION? 125

HISTORY AND MEMORY IN INTELLIGENCE 142

Marius-Răzvan PREDOANĂ, **Ana-Rodica STĂICULESCU, Bianca-Elena STAN,**
THE ROOTS AND INSTRUMENTS OF RUSSIA'S PROPAGANDA CAMPAIGN 143

PRACTITIONERS' BROAD VIEW 163

Florin BUŞTIUC, **Alexandra POPESCU (ANGHEL),**
FIŞE INTEROGATIV-EVALUATIVE ALE FACTORILOR RELEVANȚI PENTRU STRUCTURILE INFORMATIVE/DE LAW ENFORCEMENT 164

REVIEWS AND NOTES 189

Florica Dobre, *O istorie a CIE (Centrul de Informații Externe): octombrie 1978 - decembrie 1989: structuri, cadre, obiective şi metode*, Editura Glasul istoriei, București, 2022, vol 1, p. 675 și vol 2 p. 630
prezentare de Codruț LUCINESCU 190

ACADEMIC FOCUS 194

EU-HYBNET Project 195

INSET Project 197

ERASMUS+ Mobility Projects 200

Smart Cities and Regional Development Journal 202

Call for Papers Romanian Intelligece Studies Review 204

INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

THE ROLE OF HUMAN INTELLIGENCE IN THE AGE OF DIGITAL TECHNOLOGY

Domenico FRASCÀ*
Giulia VENTURI*
Maria USTENKO*
Alessandro ZANASI*
Andrew STANIFORTH*
David FORTUNE*

Abstract:
This paper focuses on the role and perspectives of Human Intelligence in the digital era. It explores technological advancements that can be harnessed by Intelligence and Security practitioners in the fields of HUMINT and its associated support activities. The paper considers various technologies, including tools for decision support, deception and information detection, and strategies for mitigating cognitive biases and other limiting factors. The analysis concerns technologies, tools and techniques used in all phases of the Intelligence Cycle, evaluating their utility considering the current challenges posed by them for Intelligence Communities and Law Enforcement Agencies. Recent developments in technologies which support other Intelligence disciplines such as SIGINT, IMINT and OSINT have potentially diminished the standing and priority of HUMINT within the Intelligence Cycle. Moreover, psychology has a crucial role in comprehending HUMINT, as human minds have their imperfections, and psychological processes like cognitive biases can result in unanticipated mistakes and unintentional outcomes within the field of Intelligence. Still, HUMINT sources continue to play a fundamental role in Intelligence Collection, analysis, and interpretation, due to their ability to recall, recognise, contextualise, and establish

* Security researcher at Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* Program manager at Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* Project manager at Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* President of Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* Director of Saher Europe OÜ, Männimäe (Estonia), e-mail: contact@saher-eu.com
* Director of Saher Europe OÜ, Männimäe (Estonia), e-mail: contact@saher-eu.com

connections between different information. HUMINT continues to be a vital element, providing a human touch and insights that can be difficult to reproduce solely through technological methods.

Keywords: *HUMINT, Intelligence, Intelligence Cycle, Security, Technology.*

Introduction

Human Intelligence (HUMINT) is an Intelligence discipline recognised by national security policymakers as the human collection of information through both overt and covert methodologies. The covert, sensitive and secretive nature of HUMINT creates difficulties when it comes to openly and publicly examining, reviewing, or researching the tools, methods, technologies, and skills involved in this confidential Intelligence-gathering field. Recent advancements in technologies supporting other Intelligence disciplines have raised questions about the standing and priority of HUMINT within the Intelligence Cycle. However, it is important to acknowledge that HUMINT sources continue to hold a critical and irreplaceable role in Intelligence collection, analysis, and interpretation. The unique abilities of HUMINT sources, including their capacity to recall, recognise, contextualise, and establish connections among diverse pieces of information, make them invaluable contributors to the Intelligence community. While technology has enhanced various aspects of Intelligence gathering, HUMINT remains an essential component, offering a human element and insights that can be challenging to replicate with technological means alone.

The aim of this paper is to illustrate the current role of HUMINT in light of the latest technological developments, as well as to provide insights to the state-of-the-art of technological advancements exploitable by Intelligence and security practitioners in the fields of HUMINT and support activities. This also encompasses any technology, tools, or methods that are presently considered to be operating beyond the accepted legal, ethical, and cultural standards of security and Intelligence policy practices and procedures in the European Union (EU). The methodology employed involves a thorough analysis of technologies from diverse viewpoints. To achieve this, it was conducted an extensive review of a range of public information sources, including EU-funded projects and related initiatives, primary publications, peer-reviewed

papers, websites, news reports, whitepapers, reference materials detailing best practices and standards, among others. Additionally, have been supplemented the newly identified technology solutions from these sources with other commercial technologies that were documented in the literature and accessible on public websites.

The basic concepts of HUMINT are explored and defined in the first section. The following sections present a review of the latest technological solutions for HUMINT activities and outline their utility considering the Intelligence requirements and security applications. Finally, this paper offers a set of recommendations and relevant discussion topics on the challenges and opportunities of HUMINT technologies for Intelligence organisations and Law Enforcement Agencies (LEAs) within the European framework.

Definition of Human Intelligence

HUMINT is a discipline that refers to Intelligence gathered through means of interpersonal contacts and human sources. Its methodologies can be overt, such as in an interview, or covert, such as through surveillance, and reconnaissance (NATO Allied Command Transformation, 2023). Although associated to the military, the term HUMINT can apply in a variety of civilian sectors, such as LEAs (Clark, 2013). Amongst the rise of other Intelligence disciplines such as Signals Intelligence (SIGINT), Imagery Intelligence (IMINT) and Open-Source Intelligence (OSINT), based on technological advancements, HUMINT remains the oldest method for collecting information, and until the technical revolution of the mid-late 20th century, it was the primary source of Intelligence (US Office of the Director of National Intelligence, 2023). The Official NATO Terminology Database defines HUMINT as "*Intelligence derived from information collected by human operators and primarily provided by human source*" (NATO Standardization Office, 2015). The NATO definition of HUMINT has been adopted and applied in this study as it provides the broadest definition and covers the international dimension of the Intelligence and security practitioners landscape which is essential as it applies to military and defence Intelligence, as well as Intelligence organisations, LEAs, and other security practitioners. Indeed, the NATO definition of HUMINT provides

a description of the discipline that generally encompasses all the definitions provided at the national level by NATO Countries and EU Member States.

For the public, HUMINT is still closely associated with espionage and secretive operations; however, most of HUMINT collection is performed by overt collectors such as strategic debriefers and military attaches (US Office of the Director of National Intelligence, 2023). Although spying and informing on others is described in Intelligence community circles as the oldest Intelligence discipline, HUMINT continues to evolve. Even though the fundamental principles of human espionage remain unchanging, several factors have shaped and redefined the principles and scope of Intelligence over time. It is not only the methods of HUMINT that have evolved but also the reasons and approaches used. Demographics, technology, and cultural expectations all contribute to shaping the modern clandestine service officer or covert HUMINT source of information for Intelligence organisations and LEAs.

HUMINT application

The operational advantages of HUMINT are extensive, and effectively employing this discipline can significantly enhance Intelligence-driven operations and investigations. Intelligence agencies recognise that HUMINT provides a deeper understanding of the context surrounding a potential threat, including the motivations, intentions, and capabilities of the individuals involved. HUMINT also offers a greater degree of flexibity as assets can be directed to focus on pressing security concerns and can be targeted to achieve coverage and reporting on specific intelligence requirements. Moreover, HUMINT offers unique insights to hard to reach areas fo intelligence collection, being able to infiltrate and expose the inner workings and planning of hostile organised crime gangs, extremist groups and terrorist cells.

The operational advantages of HUMINT are not only restricted to the traditional physical elements of intelligence gathering. The contemporary use of HUMINT has observed positive applications in reporting on matters of cyber security. For instance, HUMINT can be used to collect information about potential threats to an organisation's information systems and infrastructure, including insider threats, social

engineering attacks, or various forms of cyber-espionage (CQR Company, 2023). It is this type of information that is instrumental in developing threat Intelligence that aids in identifying and mitigating potential risks which can also be used to examine and explore vulnerabilities in an organisation's physical and digital infrastructure. By gathering information about the organisation's systems, processes, and personnel, HUMINT assists in identifying potential weaknesses that malicious actors could exploit (CQR Company, 2023).

All Intelligence disciplines have their limitations, constraints and disadvantages and HUMINT is no exception. The recruitment, training, nurturing, and ongoing management of HUMINT sources demands substantial resources in the form of time, personnel, and budget to ensure their safety, security, and to generate valuable Intelligence outcomes. Moreover, HUMINT assets need to be handled by highly skilled, professionally trained and dedicated Intelligence personnel who owe a duty of care to the safety, security and well-being of their source. The operational deployment of trained HUMINT assets in the field, being managed by highly proferssional and skilled intelligence operatives, is no gurantee of success. For instance, establishing contacts and handling agents is a time-consuming process, and source reliability and information credibility are often difficult to assess (Pigeon, Beamish, & Zybala, 2002). There are also numerous legal, ethical, and regulatory considerations. The use of HUMINT must adhere to ethical standards and comply with all relevant laws and regulations, which can restrict the scope and scale of operations. Furthermore, there is a persistent risk of exposure and jeopardising the safety and security of those involved. When coupled with the limitations related to scalability and access in high-risk situations, these factors contribute to the complexity of the discipline (CQR Company, 2023). Despite these limiting factors, HUMINT remains a crucial Intelligence discipline that can provide critical information that other Intelligence assets may not be able to deliver.

Acquisition of HUMINT sources

The HUMINT discipline encompasses a diverse set of abilities, spanning from conventional diplomatic communication to techniques involving manipulation and deception. Its central aspect involves the

capability to enlist an individual for the purposes of espionage, information gathering, and infiltration. Evaluating the trustworthiness, motivations, and truthfulness of the human source right from the initial stages of recruitment, and throughout their entire tenure as a human source, is essential for identifying deception, ensuring operational security, and averting the risk of infiltration and various insider threats that could potentially expose State secrets (US Department of the Army, 2020). Additional skill sets in HUMINT encompass counter-Intelligence, surveillance, liaison exploitation, the use of cover, and the implementation of false flag operations.

The process of acquiring an individual for the purpose of espionage and Intelligence-gathering on behalf of a State agency is commonly known as the *Recruitment Cycle*, which involves the ability to identify an individual with access to the required information, identify their vulnerabilities, and assess whether they may be receptive to a recruitment pitch, manipulate those vulnerabilities with the aim of making them more inclined to agree to the recruitment proposal, and finally secure the individual's cooperation. The recruitment of Intelligence sources is an art of its own, where the ability to detect deception is a critical skill for anyone involved in recruiting individuals to carry out specific tasks (Sano, 2015).

The acronym MICE, which stands for Money, Ideology, Compromise, and Excitement, offers a basic explanation of the core motivations and reasons for individuals to become HUMINT sources as follows:

(1) *Money:* the allure of financial gain is a potent motivator for people in general. For a potential Intelligence agent, the right financial incentive can induce them to take significant risks and share sensitive information with a foreign case officer.

(2) *Ideology*. ideologically motivated agents are often seen as particularly dangerous, especially for counter-Intelligence officers tasked with identifying double agents and traitors within their own agencies. Ideology can take various forms, including religious, political, and social affiliations. However, for a case officer, a source driven by ideology can be a potent asset.

(3) *Compromise/coercion*: in contrast to ideology, agents who are coerced or compromised into sharing Intelligence are less desirable.

An agent driven by ideology is rooted in a set of beliefs that go beyond personal interests. On the other hand, a compromised or coerced agent, typically through blackmail, is more susceptible to influence and likely to act to avoid punishment. Because they do not willingly cooperate, they may harbour negative emotions about being an agent, which can pose challenges for a case officer.

(4) *Excitement/ego*: finding ways to stroke or manipulate the human ego and the desire for excitement is a primary approach for a case officer to recruit an asset. While these two traits are often grouped together, they have some distinctions. *Excitement* is a fleeting feeling, whereas if the case officer effectively works on an individual's "ego", it can have a more enduring impact (Burkett, 2013).

Personnel involved in Intelligence, security, and LEAs who are engaged in the development, recruitment, and handling of human sources carry out a diverse array of functions to accomplish the mission of gathering information. These functions encompass both overt and covert methods for Intelligence collection, overseeing the collection and reporting processes, and directing the use of Intelligence to support various operations and investigations. The methodologies and practices employed in HUMINT tradecraft are intricate and encompass a range of tools, techniques, and technologies designed for targeting, recruiting, and utilising HUMINT sources. These practices are inherently sensitive and confidential. Furthermore, different agencies operating in distinct jurisdictions use varying tradecraft techniques, and the disclosure of these methods to the public is safeguarded through rigorous operational security measures, legal non-disclosure agreements, and, in some cases, in compliance with specific national laws and regulations (US Defense Intelligence Agency, 2008).

Technological solutions for HUMINT

Various technology solutions are available to support HUMINT activities, and some of these include tools to detect deception and address cognitive bias challenges within the HUMINT domain.

(1) "iCognative" by Brainwave Science: this technology scientifically identifies whether specific information is stored in the human brain by measuring brainwaves, specifically using the P300 brainwave response

mechanism. Unlike a conventional polygraph that detects emotional stress responses associated with lying, "iCognative" determines only the presence of information within the brain. It boasts a claimed accuracy rate of over 99% (Brainwave Science, 2023).

(2) "Paragon X" by Limestone Technologies: this data acquisition system in the polygraph domain is lauded for its performance, reliability, and innovation, offering features such as high retention USB and dual-channel 32-bit capabilities (Limestone Technologies, 2023).

(3) "CVSA III" by NITV Federal Services: a computer voice stress analyser designed for assessment and lie detection applications, "CVSA III" is known to be highly accurate and has been validated through multiple technical and scientific studies (NITV Federal Services, 2023).

(4) "Palantir Gotham and Palantir Foundry" by Palantir Technologies: this software provides Intelligence organisations and LEAs with the ability to unify and integrate various types of data, regardless of size, source, or format, while maintaining data integrity and source system classifications. It also offers tools for refining and managing high-volume datasets, as well as infrastructure for deploying, training, evaluating, and improving Artificial Intelligence (AI) and Machine Learning (ML) solutions. By enhancing human expertise with technology, it enables analysts to spend more time understanding and engaging with data (Palantir Technologies, 2023).

(5) "EyeDetect+" by Converus: this technology detects deception by monitoring and recording physiological activity, similar to a polygraph, along with involuntary eye behaviour changes during a test. It offers a less intrusive and more impartial alternative to traditional polygraph testing, providing credible assessment experts with reliable testing and valid data analysis (Converus, 2023).

(6) "MX908" by 908 Devices: it enhances the capabilities of emergency responders, bomb disposal units, and the military by enabling rapid detection, identification, and monitoring of explosives and their precursors. It is particularly useful for covert meetings and delivers exceptional selectivity and sensitivity for the identification of explosives and precursors (908 Devices, 2023).

These technology solutions for HUMINT support offer valuable insights into various aspects of the specialised and secretive field of

Intelligence gathering. They cover a wide range of topics, from practical tactics and operational management to the personal characteristics, behaviours, human factors, and cognitive and psychological elements involved in HUMINT operations and investigations. These technologies provide support across the entire HUMINT landscape. It is worth noting that some of these technologies also address physical protective security needs in the HUMINT field, including mobile explosive and precursor detection equipment. This equipment is crucial for ensuring the safe screening of venues where high-value covert HUMINT sources meet with their law enforcement, Intelligence agency, or military Intelligence handlers involved in highly sensitive operations. Furthermore, some of these technologies have applications in other Intelligence disciplines. For instance, they can be used to integrate multiple sources of data to create a more comprehensive Intelligence picture. The identification and inclusion of technologies related to voice stress recognition also have broader security applications within the Intelligence Cycle. Voice stress recognition can be employed to assess and identify stress levels in reports from the public, as well as in interviews with witnesses, criminals, and terrorists. These results can significantly enhance the value of the Intelligence being collected, assessed, analysed, and prioritised.

Deception and disinformation detection

Recognising deceptive information has become increasingly challenging, particularly in light of the uncontrollable spread of disinformation, especially on social media platforms. With news and information being widely shared, it has become increasingly essential in the Intelligence field to distinguish between truthful and deceptive information. Intelligence agencies have long focused on disinformation detection as a critical aspect of their work, as well as engaging in their own misinformation and disinformation operations to shield the true nature and intentions of their covert operations. In the recruitment phase of developing new HUMINT sources, the ability to detect disinformation and deception is a vital skill. This skill is essential for assessing risks and ensuring that recruited individuals do not have

hostile intentions or ulterior motivations that could compromise the integrity of HUMINT sources. Furthermore, ongoing assessment of the integrity of HUMINT sources during their operational deployment is a crucial component of effective source handling and management. Any advancements in deception detection tools, techniques, and technologies are of direct interest to the field of HUMINT, as they can contribute to enhancing the discipline's effectiveness in identifying and mitigating deception and disinformation.

Expert.AI, formerly known as Expert System, has developed a dedicated technique for recognising disinformation based on a technology named "COGITO" (Expert.AI, 2019). This technique combines rule-based semantic engines and ML algorithms, using a hybrid approach. The process involves extracting stylometric features from textual content, which are then used to train ML models. Computational Stylometry is a field in Computational Linguistics that focuses on analysing the literary style of text (Zheng, Li, Chen, & Huang, 2006). It uses techniques to identify various personality traits and characteristics of the author based on their writing style. These characteristics may include sociological factors like age, gender, and education level, as well as psychological factors like personality traits, mental health, and whether the author is a native speaker (Daelemans, 2013). Deceptive texts exhibit specific stylometric features that differentiate them from truthful ones. It is worth noting that stylometric analysis focuses on the unintentional choices made by the writer in their text, as these features are inherent to their writing style and cannot be easily manipulated. This approach allows for the detection of disinformation based on the unique stylometric characteristics of deceptive texts, enabling more accurate identification and mitigation of deceptive content.

Next-generation deception detection for HUMINT is incorporating non-invasive brainwave technology, such as the P300 response, which is being adopted by LEAs around the world. For instance, the Dubai Police Force recently made a significant breakthrough in a murder case by using brainwave science technology to measure the brain waves of suspects, marking a notable use of innovative neuroscience tools in crime investigations (Staniforth, 2021). The origins of P300 technology can be traced back to a discovery in 1965 when scientists observed

distinctive electrical activity in the brain occurring 300 milliseconds after a person saw something familiar during electroencephalogram tests. This response was termed "P300". While the neurological basis of this response remains unclear, P300 has been used as a foundation for Brain Fingerprinting (BF) in neuroscientific research. BF detects concealed information stored in the human brain by measuring brainwaves. P300 responds to words or images relevant to a crime scene or specific knowledge, making it a valuable tool for investigators to detect information stored in the brain, especially related to criminal activities or terrorism. The P300 deception detection technology has demonstrated resilience against deceptive tactics, making it less prone to false positives compared to traditional polygraph deception techniques. This advancement has the potential to bring significant improvements to the criminal justice system, reducing the risk of miscarriages of justice and enhancing the protection of crime victims (Staniforth, 2021).

Technology and cognitive biases in HUMINT

Psychology plays a significant role in understanding HUMINT because human minds are not without their flaws. Psychological mechanisms, such as cognitive biases, can lead to unexpected errors and unintended consequences in the realm of Intelligence. Cognitive biases are described as "patterns of deviation in judgment that occur in particular situations, leading to perceptual distortion, inaccurate judgment, illogical interpretation, or what is broadly called irrationality" (Tversky & Kahneman, 1973) or as "mental errors caused by individuals' simplified information processing strategies" (Heuer, 1999). They can affect the entire Intelligence Cycle, from data collection to processing, analysis, and dissemination: e.g., they can lead to misinterpretation of the significance of data or misattribution of causal relationships between data, they can produce too much trust in Information Technology (IT) tools. In recent years, EU research community has been actively engaged in addressing and countering cognitive biases in the field of Intelligence analysis. In particular, it has examined the relationship between cognitive biases and various phases of the Intelligence Cycle. This includes stages like planning and direction, collection, processing,

analysis, and dissemination. The findings of these studies have indicated that cognitive biases can affect analysts horizontally across all phases of the Intelligence Cycle, highlighting the importance of addressing and countering biases at every stage of the Intelligence process. This involvement is exemplified by projects such as the Law Enforcement Intelligence Learning Applications (LEILA) (European Commision, 2016) and the REduction of COgnitive Biases in Intelligence Analysis (RECOBIA) (European Commission, 2016) These projects have been instrumental in developing strategies and tools to mitigate the impact of cognitive biases on intelligence analysis.

Some examples of the reported cognitive biases include the following.

(1) "Confirmation Bias": the tendency to seek or interpret information in a way that confirms preconceptions.

(2) "Representativeness": the tendency to classify based on partial similarities to something typical or representative.

(3) "Availability Heuristic": the tendency to estimate what is more likely based on what is more available in memory, often biased toward vivid, unusual, or emotionally charged examples.

(4) "Anchoring": the tendency to rely too heavily on past reference points or a single piece of information when making decisions. Additionally, there are biases that impact specific phases of the Intelligence analysis process, such as the "Focusing Effect" and the "Illusionary Correlation": the first is the tendency to place too much importance on one aspect of an event, potentially causing errors in predicting future outcomes; the latter leads to the inaccurate perception or memory of a relationship between two unrelated events. Furthermore, the use of IT tools to process and make sense of available data has introduced significant advantages but has also amplified the effects of cognitive biases or triggered new biases (Pirolli & Card, 2005). For instance, the use of search and filtering technologies can lead to biases by assuming that collected data genuinely reflect reality or perceiving a data set as complete, which may lead to a cessation of further investigation.

To mitigate the impact of cognitive biases, a variety of software tools and technological solutions are at the disposal of analysts. Some of

these technologies automatically display large volumes of information in various formats, allowing analysts to efficiently explore and examine data. Additionally, visualisation tools aid analysts in making more rapid and accurate inferences by revealing patterns and connections in the data. Other tools are adept at uncovering relationships between events across time and space, as well as identifying interconnections among various entities, such as individuals, organisations, locations, and dates. This category encompasses a wide range of tools, including those supporting structured analytical techniques, Decision Support Systems (DSS), Group Support Systems (GSS), collaborative analysis tools, serious games, data mining tools, statistical software, text mining tools, and risk analysis software. Collectively, all these tools and solutions play a critical role in minimising the impact of cognitive biases in the field of Intelligence analysis, enabling analysts to provide more objective and well-informed assessments.

The role of HUMINT in the digital era: discussion and recommendations

The landscape of the Intelligence gathering has indeed seen significant transformations due to technological advancements, which have raised questions about the standing and priority of HUMINT in the Intelligence Cycle. These advancements have the potential to diminish the value of HUMINT, particularly in an age of high-tech surveillance and widespread use of social media for instant mass communication. New AI-powered surveillance platforms, combined with emerging bio and facial recognition technologies, have created a challenging environment for covert HUMINT sources operating in public spaces. The proliferation of private security and advanced Closed-Circuit Television (CCTV) digital systems further increases the risk of source compromise, making the collection of HUMINT more challenging. Technology is now not only used for surveillance but also for counter-surveillance of potential targets and HUMINT sources. This includes monitoring online activities, tracking movements through Global Positioning System (GPS), and other forms of electronic surveillance. As a result, the gathering of HUMINT has become increasingly digital and

virtual. HUMINT handlers are adopting new developments in encrypted digital communications to mitigate these risks.

Technology facilitates communication between human sources and Intelligence operators, regardless of their physical locations. This includes the use of encrypted messaging, email, video conferencing, and other forms of online communication. While technology has presented challenges to traditional HUMINT, it also offers opportunities for more secure and efficient communication between sources and Intelligence personnel.

The use of new technology for surveillance may initially frustrate HUMINT operations by potentiailly compromising the identity of the informant or the location of covert meetings, but the Intelligence community responds by introducing, implementing, and integrating tools, techniques, and technologies to counter these challenges. Technological advancements have a profound impact on both HUMINT and the broader Intelligence Cycle. For instance, technology is instrumental in analysing vast volumes of data, which includes information collected through HUMINT operations. Advanced analytical techniques, such as ML, are employed to identify patterns and anomalies that might signify potential security threats. Furthermore, technology is used to collect, store, and manage HUMINT data, encompassing digital records, images, and various types of information. Secure databases and other information management systems are used to uphold the confidentiality and integrity of this data. In addition, technology is applied for biometric identification of individuals, including facial recognition and fingerprint scanning, to support the identification of potential targets and threat actors. The continuous integration of technology enhances the capabilities of Intelligence agencies and their ability to respond to evolving security challenges.

HUMINT indeed holds substantial value in the realm of information security, with a particular focus on threat Intelligence, incident response, and cybercrime investigations. It provides critical information and insights that may not be accessible through technical means alone, contributing to enhanced effectiveness and efficiency in information security efforts. As cyber threats grow in sophistication and

complexity, the need for HUMINT to complement technical measures is likely to become even more crucial. In essence, the utilisation of HUMINT in information security, whether for public authority services or private sector businesses, is expected to maintain its significance. Moreover, as AI and automation continue to expand their roles in information security, the discipline of HUMINT may become even more valuable in identifying and mitigating emerging threats. A well-balanced integration of technical capabilities and human resources is essential for effectively utilising HUMINT in information security. By harnessing the strengths of both approaches, security organisations, Intelligence agencies, and LEAs can enhance their ability to safeguard themselves and their stakeholders from the ever-evolving threats in the digital landscape.

Conclusions

The increased digitisation of the Intelligence gathering discipline has raised concerns among some national security policymakers. They have criticised defence, Intelligence organisations, and LEAs for appearing to deprioritise, under-resource, or neglect HUMINT in favour of more readily accessible sources of information. In the past decade, the proliferation of affordable, sophisticated high-tech surveillance technology has expanded globally, particularly in the realms of audio and video surveillance. Consequently, there has been a perception that the value and contribution of HUMINT to the overall Intelligence landscape have been diminished. To some extent, the widespread availability and decreasing cost of surveillance and public monitoring technology have led to increased investment and reliance on remote Intelligence collection through modern technological disciplines like SIGINT and IMINT. Additionally, the growth of OSINT, which involves Intelligence derived from publicly available information, has enriched the capabilities of LEAs. OSINT provides access to actionable Intelligence, enhancing decision-making, tasking, and coordination activities. The concerns raised by national security policymakers underscore the evolving nature of Intelligence gathering and the need for a balanced approach that leverages both traditional HUMINT methods and contemporary

technological Intelligence disciplines to address the complex and multifaceted challenges in the digital age.

The relentless pursuit of Intelligence to understand new and emerging threats has fuelled the growth of OSINT as a vital intelligence discipline in the digital age. However, the increasing availability of publicly accessible information should not diminish the value, standing, and investment in HUMINT. To effectively prevent various contemporary security threats, avoid strategic surprises, and unveil what hostile actors seek to keep hidden, security operations must remain Intelligence-led and include HUMINT as an integral component. In light of this, HUMINT retains a crucial role in informing the Intelligence Cycle. While recent advancements in ubiquitous surveillance have presented new challenges, there is a need to ensure that HUMINT remains relevant and effective in the digital age. One important step is to review current HUMINT doctrine to align it with the strategic Intelligence requirements of government agencies, ensuring the safety and security of EU Member States. Balancing HUMINT with other Intelligence disciplines is also essential for addressing the evolving threat landscape comprehensively.

Acknowledgement: This work was supported by the NOTIONES (iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS) project, that has received funding from the European Unions' Horizon 2020 research and innovation programme under grant agreement No. 101021853. The objective of the NOTIONES project is to build a pan-European network of practitioners from the security and Intelligence services, from the industry – including SMEs – and from the Academia, with the objective to enhance their interaction and identify specific technology and innovation requirements, needs, expectations and gaps.

References:

1. 908 Devices. (2023). MX908. Retrieved September 12, 2023, from 908 Devices, https://908devices.com/products/mx908/.

2. Brainwave Science. (2023). iCognitive. Retrieved September 12, 2023, from Brainwave Science, https://brainwavescience.com/icognative/.

3. Burkett, R. (2013, March). "Rethinking an Old Approach. An alternative Framework for Agent Recruitment: From MICE to RASCLS." *Studies in Intelligence*, 57(1), 7-17. Retrieved September 4, 2023, from https://www.cia.gov/static/Alt-Framework-Agent-Recruitment.pdf.

4. Clark, R. (2013). *Intelligence Collection*. Washington, D.C., USA: CQ Press.

5. Converus. (2023). *The World's First Automated Polygraph: EyeDetect+.* Retrieved September 12, 2023, from Converus, https://converus.com/eyedetectplus/.

6. CQR Company. (2023, February 14). *HUMINT*. Retrieved September 5, 2023, from CQR Company, https://cqr.company/pentesting-process/humint/.

7. Daelemans, W. (2013). "Explanation in Computational Stylometry." In International Conference on Intelligent Text Processing and Computational Linguistics (pp. 451-462). Springer. Retrieved September 10, 2023.

8. European Commision. (2016, December 5). *Law Enforcement Intelligence Learning Application*. Retrieved September 6, 2023, from European Commission, https://cordis.europa.eu/project/id/608303.

9. European Commission. (2016, February 18). *REduction of COgnitive BIAses in Intelligence Analysis*. Retrieved September 6, 2023, from European Commission, https://cordis.europa.eu/project/id/285010#:~:text=Objective,affect%20the%20practice%20of%20intelligence&text=%2D%20organization.

10. Expert.AI. (2019, March 19). *Expert System Annuncia la Nuova Versione della Piattaforma di Intelligenza Artificiale COGITO*. Retrieved September 10, 2023, from Expert.AI, https://www.expert.ai/it/expert-system-annuncia-la-nuova-versione-della-piattaforma-di-intelligenza-artificiale-cogito/.

11. Heuer, R. (1999). *Pyschology of Intelligence Analysis.* Retrieved September 5, 2023, from Central Intelligence Agency, https://www.cia.gov/static/Pyschology-of-Intelligence-Analysis.pdf.

12. Limestone Technologies. (2023). *Polygraph Pro Suite Products.* Retrieved September 12, 2023, from Limestone Technologies, https://limestonetech.com/polygraph-pro-suite-products/.

13. NATO Allied Command Transformation. (2023, July 10). *NATO Centres of Excellence – Human Intelligence.* Retrieved September 4, 2023, from NATO

Allied Command Transformation, https://www.act.nato.int/article/nato-coes-humint/.

14. NATO Standardization Office. (2015, August 20). *HUMINT.* Retrieved September 4, 2023, from Official NATO Terminology Database, https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en.

15. NITV Federal Services. (2023). *CVSA III*. Retrieved September 12, 2023, from NITV Federal Services, https://www.cvsa1.com/products.htm.

16. Palantir Technologies. (2023). *Intelligence*. Retrieved September 12, 2023, from Palantir Technologies, https://www.palantir.com/offerings/intelligence/.

17. Pigeon, L., Beamish, C., & Zybala, M. (2002, September). Pigeon, L., Beamish, C.J., & Zybala, M. (2002). *HUMINT Communication Information Systems for Complex Warfare.* Retrieved September 12, 2023, from 7th International Command and Control Research and Technology Symposium (ICCRTS 2002), https://apps.dtic.mil/sti/pdfs/ADA467646.pdf.

18. Pirolli, P., & Card, S. (2005, May). "The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis." Proceedings of International Conference on Intelligence Analysis, 5(1), 2-4. Retrieved September 5, 2023.

19. Sano, J. (2015, Fall/Winter). "The Changing Shape of HUMINT Guide to the Study of Intelligence." *AFIO Intelligencer Journal*, 21(3), 77-80. Retrieved September 4, 2023, from https://www.afio.com/publications/SANO%20John%20on%20The%20Changing%20Shape%20of%20HUMINT%20Pages%20from%20INTEL_FALLWINTER2015_Vol21_No3_FINAL.pdf.

20. Staniforth, A. (2021, March 25). *Murder Investigation: The Police Application of Brainwave Technology*. Retrieved September 12, 2023, from Policing Insight, https://policinginsight.com/features/innovation/murder-investigation-the-police-application-of-brainwave-technology/.

21. Tversky, A., & Kahneman, D. (1973, September). "Availability: A Heuristic for Judging Frequency and Probability." *Cognitive Psychology*, 5(2), 207-232. Retrieved September 5, 2023.

22. US Defense Intelligence Agency. (2008, March). *A Tradecraft Primer: Basic Structured Analytic Techniques*. Retrieved September 5, 2023, from US Defense Intelligence Agency, https://www.dia.mil/FOIA/FOIA-Electronic-Reading-Room/FileId/161442/.

23. US Department of the Army. (2020, January). *Intelligence Analysis (ATP 2-33.4).* Retrieved September 5, 2023, from Federation of American Scientists: Intelligence Resource Program, https://irp.fas.org/doddir/army/atp2-33-4.pdf.

24. US Office of the Director of National Intelligence. (2023). *What Is Intelligence?* Retrieved September 4, 2023, from US Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

25. Zheng, R., Li, J., Chen, H., & Huang, Z. (2006). "A Framework for Authorship Identification of Online Messages: Writing-Style Features and Classification Techniques." *Journal of the American Society for Information Science and Technology*, 57(3), 378-393. Retrieved September 10, 2023.

(COUNTER)BALANCING THE WEST: RUSSIA'S INFLUENCE IN THE WESTERN BALKANS SINCE THE END OF COLD WAR

Sanja TEPAVCEVIC*

Abstract:
Focusing on countries remnants of former Yugoslavia, this article traces sources of Russia's influence in the region, departing from the idea that these sources are of political-diplomatic, military, economic, and socio-cultural nature. Revealing the manner in which Russia uses its influence leverages in the Western Balkans, the article relies on an extensive qualitative data collected through a variety of sources including scholarly literature on the topic, statements of political leadership, interviews and informal conversations with Russian and regional decision-makers directly involved in negotiation processes, official documents, mass media reports, and social media groups and discussions. Led by the question of in what ways and to what extent has Russia influenced the post-Yugoslav region, the article sheds the light on usually overlooked aspect of Russia's influence on the relations between the republics of former Yugoslavia in the first two decades of twenty-first century. The article closes with the analysis of effects of Russia's full-fledged 2022 invasion in Ukraine on the intensity and nature of its influence in the Balkans.

Keywords: *Post-Soviet Russia, Former Yugoslavia, Influence, Foreign Policies*

Introduction: Situating Russia's Influence in Former Yugoslav Space

At the turn of the 21st century, Europe faced two parallel and opposite processes. The first was the demise of the Socialist bloc and the Soviet Union (SU) as the bloc's leader. The second process was the

* Adjunct Professor in International Studies Master Program, Faculty of Modern Philology and Social Sciences of the University of Pannonia, and Associate Researcher of the Institute of Advanced Studies Koszeg, Hungary, email: sanja.tepavcevic@gmail.com.
I would like to thank the journal's editor and two anonymous reviewers, whose comments on the article helped sharpen the argument.

integration of the European Economic Community into the political bloc – the European Union (EU) (Tepavcevic, 2021 a). The violent breakup of the Socialist Federal Republic Yugoslavia (SFRY), the only socialist European country that was not member of the Soviet bloc, reflected and paralleled these two processes. Yugoslavia existed between 1918 and 1992 as a federal state of six predominantly South Slavic republics. Most of the former Yugoslav republics, with the exception of Slovenia, were not ethnically homogeneous nation-states: Croatia had a large autochthonous Serb minority and less numerous Italian, Hungarian and Slovenian minorities, while Bosnia and Herzegovina had Bosnian Muslim, Serb, and Croat dominant communities. Serbia, the largest among Yugoslav republics, had two autonomous provinces, Vojvodina and Kosovo, which had notably different ethnic structures from Serbia's central regions: Albanian majority in Kosovo, and various ethnic groups in Vojvodina (Kovacevic-Bielicki, 2017).[1]

The first multi-party elections held in the 1990 in the country that formerly was ruled by the single – Yugoslav Communist – party, brought to power right-wing nationalist forces that called for independence and separation as a mobilizing principle in the majority of the republics. Simultaneously, many of left-wing politicians were against the separation and dissolution. Though acting as a right-wing political force, Serbian leadership associated with the left-wing politicians, opposing the dissolution. While other republics encountered violent conflicts on their territories, Federal Republic of Yugoslavia (FRY) constituting of Serbia and Montenegro, the only two republics that, until 2006, remained in the state union, also experienced significant ethnic tensions and sporadic violence in many parts of their own territories (Kovacevic-Bielicki, 2017). In 2008, Albanian majority declared Kosovo's independence from Serbia, yet, its' status as an independent state has not been fully internationally recognized and resolved by the time of writing.

Russia's influence in the post-Yugoslav space had provoked fierce scholarly discussions, consisting of two major aspects. The first aspect is

[1] The pre-war population census in Bosnia and Herzegovina from 1991 estimates that the population consisted of 43.47 percent of Bosnian Muslims, 31.21 percent of Serbs, and 17.38 percent of Croats. Source: G. Bilten (1991). Ethnic composition of Bosnia-Herzegovina population. Sarajevo: Zavod za statistiku Bosne i Hercegovine.

related to the foreign policies of Yugoslavia's successor countries towards Russia; the second aspect refers to Russia's foreign policy towards the Balkans since the 1990s. This article is led by the following question: in what ways and to what extent has Russia influenced the post-Yugoslav region between 1991 and 2022? By answering this question, the article also sheds some light on usually overlooked aspect of Russia's influence on the relations between the republics of former Yugoslavia in the first two decades of twenty-first century.

Therefore, this article traces sources of Russia's influence in the region over the last three decades, departing from the idea that these sources are of political, military, economic, and historical nature. Revealing interconnections between these sources, on the one hand, and, on the other, aspects of Russia's influence across former Yugoslav republics. The article relies on an extensive qualitative data collected through a variety of sources including scholarly literature on Russia's influence in the Western Balkans, Russia's Foreign Policy Concepts since 1992, statements of political leadership, interviews and informal conversations with Russian and regional decision-makers, mass media reports, and social media groups' discussions. The article proceeds as follows. The first section analyses scholarly discussions on Russia's global role in the post-Soviet period in general, and its' influence in the countries of former Yugoslavia in particular. The second section reflects on the place devoted to Russia in foreign policies in four geographically central former Yugoslav republics. The third section analyses the place of the Western Balkans in Russia's post-Soviet foreign policy tracing Russia's role in the countries resulted from Yugoslavia's disintegration through the three decades – the 1990s, 2000s, and 2010s. The paper closes with the analysis of effects of Russia's full-fledged 2022 invasion in Ukraine on the intensity and nature of its influence in the Western Balkans and drives some conclusions.

Russia's Influence in Europe – Scholarly Discussions

Scholarly literature on Russia's influence abroad evolves across four major themes. The broadest theme is Russia's international image, or the way in which Russia is perceived globally. As the largest and central republic of the former world's second military superpower, the

SU, its' legal successor in international organizations, territorially the world's largest country, for most of the thirty years after the Soviet demise, Russia has largely been perceived as imperial expansionist (Tepavcevic, 2013). Simultaneously, Russia emerged as a key global economic player as the largest exporter of oil and gas (Stent, 2008), combined with assertive foreign policy rhetoric of its political leadership contributed to these perceptions.

However, a closer view suggests that Russia means different things in different periods, and in different contexts during the same period (Neumann, 1998). First, Russia's historical legacy in post-Soviet neighboring countries as well as in Central and Eastern Europe (CEE) from Soviet times, and its political system, have left many countries hostile to Russia (Neumann, 1998; Abdelal, 2005; Orban, 2008). In contrast to CEE, Yugoslavia's successor states did not join military and political blocs in Europe during the Cold War. Therefore, they did not share these negative experiences and, consequently, the same fears as their CEE neighbors, though they have similar goals of joining the EU (Tepavcevic, 2015; Reljic, 2009). Therefore, this strand of literature suggests the proposition that Russia's influence in Europe and particularly in the Western Balkans is a consequence of Russia's historical legacy among the population of these countries. These works display Russia mostly as a military power.

Following the argument of historical legacy, many authors focused on foreign and economic policies of other countries as agents in international relations. For instance, Abdelal (2005) suggested that economic policies in other post-Soviet republics were formulated and implemented in accordance to their national identities, while these identities were formulated in relation to Russia. As a result, for instance in Lithuania, Russia's image as the significant 'other' was, in the eyes of the decision makers in economic policy, a decisive factor in their choice of a liberal path in Lithuanian economic policy and foreign policy orientation. At the same time, among the Belarussian political elite, Russia's image as the country's only supplier of energy had exactly the opposite effect in shaping the republic's post-Soviet economic and foreign policies (Abdelal, 2005). This discussion provides the general proposition that Russia is very influential in economic and foreign policy

decision-making in other post-socialist countries. Therefore, this strand focuses on Russia as a state, owning significant resources to influence politics and foreign policies of neighboring countries.

The third broad theme in scholarly literature has concerned Russia's economic influence through outward investments of Russian companies. In this context, Kuznetsov (2007) pointed out that Russian investments were not welcomed in developed countries, while developing countries usually tended to attract the investments of Russian companies. Building upon such argument, Tepavcevic (2018) demonstrated that the reaction of local authorities and business communities to investment by Russian state-owned energy companies and banks particularly in Hungary and Serbia were mostly shaped by the level of a host country's international position and economic development, rather than by Russia's foreign policy interests and goals. In this context, attempts to attract Russian companies' investments seemed particularly striking in Serbia, and in the Serb political entity of Bosnia and Herzegovina, officially known as Republika Srpska (Tepavcevic, 2015 and 2018). Therefore, these works postulate that the economic interests of the aforementioned countries and political entities shaped their foreign policies towards Russia.

The last proposition develops the theme of the influence of Russian companies' investment abroad, including Yugoslavia's successor states, as an aspect of Russian interests. This proposition is also the most influential. The authors representing this strand of discussion portray post-Soviet Russia's economic influence as a continuation of pursuing state interest by 'softer' means, thus, approaching Russian state-owned energy companies as new agents of Russia's political influence (Orban, 2008; Nygren, 2007). As such, Tsygankov (2006) suggested that the post-Soviet Russia largely inherited foreign policy aspirations of the SU. According to him, the post-Soviet government exchanged its foreign policy strategy for soft power, or, in other words, it applies coercion "by banks" rather than coercion "by tanks". Therefore, this strand also emphasizes the role of Russian companies as actors shaping Russia's influence in Europe. In sum, the literature offers four propositions as demonstrated in Table 1 below.

Table 1. Propositions about Russia's influence (Source: author's view based on literature review)

Proposition	Interest in focus	Sphere of Influence
Geopolitical: Russia as a political factor is influential in economic and foreign policy decision-making in other post-socialist European countries	Political interests of Russia and other countries	Economic and foreign policy – influencing either cooperation or disengagement with Russia, or Russia with other countries
Economic needs of other countries: the economic needs of countries shaped their policies regarding cooperation with Russia.	Other countries' economic interests in relation to Russia	Economy
Historical: Russia's influence in Europe and particularly in the Western Balkans is a consequence of the historical experiences of Russia with the population of these countries.	Other countries' security interests in relation to Russia	Geopolitics
Geoeconomic: Russian – mostly state-owned energy – companies represent agents of Russia's foreign policy influence.	Russia's interests in relation to other countries	Geoeconomics

The next section reflects on post-Yugoslav republics' foreign policy interests in relation to Russia.

Russia in Foreign Policies of the Former Yugoslav States

Foreign policies of the Western Balkan states, as initially conceptualized former Yugoslavia minus Slovenia and plus Albania, "do not reflect their strategic national interests. (…) all Western Balkan countries could be defined as small states, despite the fact that within the region some of them are considered as being comparatively large and strong" (Rasidagic, 2013). This notion of relatively large and strong primarily refers to Serbia, which, even after Kosovo's factual secession, remains the largest in the region in terms of territory and population.

At a smaller extent, this relative regional strength refers to Croatia. Rasidagic (2013) also suggests that [T]he potential for formulation and implementation of foreign policy in all of these states is very low, due to a number of reasons (…) small territories and population, weak economies, unfinished democracy building processes, and a generally unsettled situation, typical of transitional societies. All these aspects make states in the region, to a large extent, dependent on the interests of bigger powers, as well as susceptible to policies of the international organizations ... . Western Balkan states, therefore, to varying extents, identify their foreign policies with the policies of different external actors (Rasidagic, 2013).

Indeed, a number of factors influenced Yugoslavia's successor countries to ally with a particular big power, though these alliances were diverse on various levels and topics. Nevertheless, one feature common to all these countries is that European integration has remained a top foreign policy priority. This priority was founded primarily on the geographical proximity principle, which also generated economic dominance of the EU in the Western Balkans region. In 2023, these countries reached different stages of integration: for instance, Croatia has reached full EU membership since 2013, Montenegro became an EU candidate in 2010, Serbia received EU candidate status in 2012, and Bosnia and Herzegovina received EU candidate status only in 2022. In this line of thought, I consider illustrative Serbia's Ministry of Foreign Affairs (MFA), the largest country of Yugoslavia's successors, whose website states that European integration and membership in the European Union represent the national interest and strategic commitment of the Republic of Serbia, and the European Union values are the same ones which the Republic of Serbia supports and strives to refine (...) The European Union is also the most important trade and investment partner of the Republic of Serbia, and a very important factor in the economic stability of the country (Serbia's Ministry of Foreign Affairs, 2022).

At the same time, in Serbia's foreign policy, the bilateral relations with Russia, sorted in alphabetical order, seem to occupy an important place. Bilateral relations between the Republic of Serbia and the Russian Federation are based on a strategic partnership based on a deep mutual feeling of friendship, centuries-old history of relations and the tradition

of linguistic, spiritual and cultural closeness of the fraternal peoples of the two countries. The dynamics of contacts at the highest level between officials of the two countries is intense (Serbia's Ministry of Foreign Affairs, 2021).

As this statement on Serbia's MFA website suggests, the EU integration involves pragmatic aspects of the relations, namely national interests and strategic priorities – which confirms the economic proposition. Simultaneously, the relations with Russia seem to be primarily grounded on historical, cultural and even emotional – namely the "feeling of friendship" – factors, directly confirming the proposition of Russia's historical legacy in relations with Serbia.

For Croatia, which has been an EU member state for a decade, the EU integration processes have remained top foreign policy goals. As the following statement from Croatia's Ministry of European and Foreign Affairs (MEVP abbreviation in Croatian) website suggests,

Celebrating the 10th anniversary, we are pleased to highlight that Croatia has fulfilled two strategic goals – joining the eurozone and the Schengen Area, making it one of only 15 countries that are simultaneously member states of NATO, EU, eurozone and the Schengen Area (Croatia's Ministry of European and Foreign Affairs, 2023).

While, similar to Serbia's MFA website, the bilateral relations section on Croatia's MEVP website is sorted in alphabetical order, in contrast to Serbia's MFA website, these relations are specified in tables demonstrating titles and types of bilateral agreements, the dates of their implementations and terminations. The same principle holds for Croatia's relations with Russia, and they do not contain any interpretations. Nevertheless, in particular issues, Croatia's foreign policy towards Russia traditionally follows mainstream EU stance. This is particularly striking concerning the EU stance towards Russia's 2022 full-fledged invasion in Ukraine. As stated in the Croatia's MEVP website: "The values on which the EU rests – unity and solidarity, which Croatia strongly advocates, are particularly important amidst the aggression on Ukraine, when security and energy stability of the entire European continent are topical issues" (Croatia's Ministry of European and Foreign Affairs, 2023). Therefore, Croatia's foreign policy towards Russia is part of the broader EU policy and it does not reflect any specific interests in bilateral

relations, extending the economic proposition towards a broader political one in relation to the EU membership.

Similar to Serbia and Croatia, Bosnia and Herzegovina's foreign policy was primarily focused on the preservation of independence and peace, and the EU integration. Simultaneously, in some contrast to both Serbia and Croatia, Bosnia and Herzegovina's foreign policy regional and bilateral priorities since 2003 were formulated in the section titled "Basic directions and activities of BiH foreign policy" as follows: Promotion of cooperation with neighboring countries – Republic Croatia (RC) and Serbia and Montenegro, on the basis of common interest and principles of equality, mutual respect and respect for sovereignty and territorial integrity (…) Bosnia and Herzegovina will develop bilateral relations in particular with the member countries of the Peace Implementation Council Steering Board, with the USA, Russian Federation, Great Britain, France, China and other member countries of the UN Security Council, member countries of the European Union, countries in the region, member countries of the Organization of Islamic Conference and with other countries (Chairman of BH Presidency Paravac, 2003).

However, the newest official document – 2018-2023 Foreign Policy Strategy of Bosnia and Herzegovina – notes radical changes in the international arena, including: effects of the Arab Spring, Brexit, Croatia's joining the EU, Montenegro's joining NATO, and "cooling the relations with Russia" (Bosnia and Herzegovina Government, 2018 - 2023). In such context, Bosnia and Herzegovina's foreign policy priorities remain the integration in the EU, security in cooperation with NATO, and cooperation with the neighboring countries.

Despite being a small country of only 500.000 permanent inhabitants, Montenegro is worthy to be analyzed as one of two longest-standing Yugoslavia's republics. Being in federation with Serbia until 2006, Montenegro followed the FRY foreign policy interests and goals by signing Free Trade Agreement with Russia, Belarus and Kazakhstan in 2001. Since the peaceful 'divorce' with Serbia in 2006, Montenegro pro-actively pursued EU integration, firstly, by unilaterally introducing Euro as a national currency in 2002, without a previous agreement with the EU in this respect, while the EU expressed its reticence regarding this

decision. Secondly, Montenegro joined NATO in 2017: for the majority of newer EU member states, the NATO membership closely preceded acceptance to the EU full membership. In terms of foreign policy priorities, Montenegrin Government website devoted to foreign policy affairs stated the following: Our goal is further improvement of bilateral relations with countries of the Region (…) upgrading the bilateral relations with EU countries (…) dialogue on high level, intensive cooperation in various fields, including also cooperation in respect to further affirmation of Montenegrin integration in EU, and active cooperation within NATO alliance. (…) We are focused on further implementing of determined foreign policy in bilateral relations with countries of North and South America (Montenegro's Ministry of Foreign Affairs, 2023).

Notably, the text did not mention Russia separately: instead, there is mention of Eurasia as a region. Therefore, while Serbia and Bosnia and Herzegovina, along with their EU integration agendas and the priority pivoted in the Western Balkan region, seem to have followed balanced foreign policy towards Russia, Croatia, and more recently, Montenegro have oriented their foreign policies on the EU, and, in the case of Montenegro, toward Americas.

In sum, the analysis in this section has revealed four images of Russia in the region. The first is Russia as friend noted in Serbia's official foreign policy. The second image portrays Russia as a distant security threat. It is reflected in Croatia's protocoled and highly technical report on the relations with Russia equal as with other countries outside the EU. The third image is Russia as one of the many countries in Eurasia, reflected in the "silence" about Russia in the present foreign policy of Montenegro. The fourth image is Russia as an important distant power that is presented in the Foreign Policy Strategy of Bosnia and Herzegovina. Such approaches suggest a certain insignificance of Russia in Croatia and Montenegro as compared to the EU, a certain influence of Russia in Bosnia and Herzegovina, especially significant in Serbian Republic, also in comparison to the EU, US, but also China and Islamic states, and significant influence of Russia in Serbia as against the EU. This proposition about Russia's influence focused on these four Yugoslavia's successor states is examined in the next section.

The Western Balkans in Russia's Foreign Policy: Tracing Russia's Influence in the Western Balkans in 1991-2022

Russia's Role in Wars of Yugoslavia's Dissolution: The first of Russia's post-Soviet Foreign Policy Concept (The Concept) was issued in late 1992, under President Boris Yeltsin and the notably liberal Minister of Foreign Affairs (MFA), Andrey Kozyrev, and it does not mention Yugoslavia and its successor states separately, but only in a broad context of post-socialist Central and Eastern Europe. The Concept, however, thoroughly discusses the vision of post-Soviet Russia's relations with the post-Soviet republics, the United States of America (USA), Western Europe, and countries of Central-Eastern Europe. The later were seen as a region of turbulence and in search for identity, and former members of the Soviet bloc. It also underlined post-Soviet Russia's democratic statehood and its pivotal role in international cooperation and peace (Ministry of Foreign Affair of the Russian Federation, 1992). This suggests that the Western Balkans had a very peripheral meaning for Russia's foreign policy in the early 1990s, and such a position was conditioned by Russia's government attempts to establish new relations as a state, independent from the SU, rejecting both political and geoeconomic propositions.

Following Russia's foreign policy oriented towards integration in the West during Yeltsin's first presidential term, similarly to the majority of its Western partners, by the summer 1992, Russian leadership recognized the independence of Slovenia, Croatia, and Bosnia and Herzegovina from Yugoslavia. Additionally, due to domestic economic and political weakness, Russia's leadership tried to avoid strains with the West; thus, in several instances, it supported US-led actions against Serbs. First, in 1992, it supported the initiative of the UN Security Council to use military force in Bosnia and Herzegovina to guarantee the delivery of humanitarian aid; and secondly, during the 48th General Assembly session of the UN, it voted to expel Federal Republic Yugoslavia (the union of Serbia and Montenegro) from the UN. In this alignment with the mainstream international opinion on the wars of Yugoslavia's dissolution, shaped by Russia's economic dependence on Western financial aid, Russia's leadership was not able to provide support to the Serbs. Therefore, despite the pressure of increasing nationalist mood

among the Russian society, Russian foreign policy in the Western Balkans had no influence under Yeltsin's leadership (Tepavcevic, 2013). The fact that NATO air strike on Serbs' artillery positions near Bosnian town of Gorazde in 1994 were conducted without even consulting Moscow best illustrated Russia's relative insignificance in these conflicts.

However, these strikes marked a certain turning point in Russia's stance towards the sides in Yugoslav wars: Russian leadership protested against NATO's action, blaming not only the Serbs' leadership in escalation of the conflict, but also Bosniaks and Croats. As a result, as Donaldson and Nogee (2005) pointed out, "[T]he locus of diplomatic efforts became a group of five nations – Russia, the United States, France, Great Britain and Germany – known as the "contact group". Their goal was to devise a political solution to the Bosnian civil war". These efforts in December 1995 resulted in the Dayton Peace Accords, defining the internal organization of Bosnia and Herzegovina in two major entities – The Federation of Bosnia and Herzegovina (inhabited mostly by Bosniaks and Bosnian Croats), and Srpska Republic (mainly inhabited by Serbs).

In addition, during the 1990s, Russian political leadership and armed forces were also involved in the conflict between Kosovo's Albanians and Serbs over attempts of the former to secede Kosovo from Serbia, and efforts of the latter to prevent this secession. While in this conflict, Kosovo's Serbs enjoyed the full support of the Serbian police and army, the US and the Western European powers attempted to defend the Kosovo's Albanians as they initially represented the weaker side of the conflict. In the spring of 1999, these attempts to defend Kosovo's Albanians turned into the three months long NATO's air attacks on Serbia and Montenegro (Tepavcevic, 2022b). For these attacks, as Yesson (2000) pointed out, Russian leaders accused NATO states of violating norms of sovereignty and undermining the UN Charter. In addition, the fact that these attacks were conducted without Russia's agreement signaled the need for a change in Russia's foreign policy. This was among the reasons for Yeltsin's decision to resign and to propose Vladimir Putin as his successor.

Post-Yugoslav-Wars Recovery: Russia's Foreign Policy Concept issued in 2000, under the first presidency of Vladimir Putin, and during

MFA leadership of Igor Ivanov, prioritized relations with the Commonwealth of Independent States (CIS), then with Western Europe – most notably with Germany. It also explicitly mentioned not only the Balkans as a region in the post-socialist Europe as the third priority for Russia, but also FRY, and its territorial integrity as meaningfully concerning Russia's interests in the Balkans. FRY also became the only country outside the CIS signing Free Trade Agreement with Russia. These two factors – territorial integrity of FRY and Free Trade Agreement – demonstrated a much higher significance of the post-Yugoslav space in Putin-led Russia's foreign policy. Such change in the position in The Concept towards the Balkans was conditioned by the violent conflicts of Yugoslavia's dissolution and the position adopted by Russia in this respect, which was opposed to the one taken by the USA and the Western European countries, as discussed in the following sections. Simultaneously, both political and geoeconomic propositions regarding Russia's interests of influence in the Balkans find some confirmation particularly concerning Serbia and Montenegro, as successors of SFRY. Apart from The Concept, this period was also the one in which Russia issued other significant national security related documents, such as the Military Doctrine and the National Security Concept.

Russian foreign policy during Putin's first and second presidential terms (2000-2008) in general and towards the Western Balkans in particular appeared more pragmatic than the one during Yeltsin's rule. First, in 2001, Russia and FRY signed the aforementioned Free Trade Agreement, which allowed Yugoslav companies to trade with Russia on equal conditions as the CIS countries. According to the Trade Chamber of the Srpska Republic, this Agreement also facilitated exports of some products from the Srpska Republic to Russia, where Serbian companies served as mediators. According to the representatives of former Yugoslav business community in Russia, some Croatian private companies also used Serbian companies as mediators to trade their products in Russia in more favorable conditions (personal communication with companies' official representatives, June 2005). These developments made Serbia to function as a hub for exports to Russia for the whole region (Tepavcevic, 2022b). According to representatives of Bosnian Embassy in Russia, to improve direct economic relations, in 2004,

Russia and Bosnia and Herzegovina established an intergovernmental commission for trade and economic cooperation (personal communication, July 2012).

Second, Russian companies have expanded in the countries set apart from former Yugoslavia and the Balkans in general since mid-2000s. According to the representative of the Bosnian Foreign Investment Promotion Agency (FIPA), seven companies with Russian capital over 50,000 euros invested in Bosnia and Herzegovina in 1994-2010 (online interview, November 2012). For instance, by 2011, Russia was the fifth largest investor in Bosnia and Herzegovina after Austria, Serbia, Croatia and Slovenia, and in 2011, it improved up to the fourth position mostly because the oil company Zarubezhneft's acquisition of the Optima Group in Serbs' Republic conducted in the end of 2007 (Tepavcevic, 2015). As a representative of the Trade Chamber of Srpska Republic suggested, Russian investors in Optima Group were preferable to the Western European ones.

There was one attempt by the British company 'Vitol' to privatize the Refinery, but the attempt was fraud as the investor did not want to purchase on minimal acceptable for Serbs' Republic price. As a result, the former Refinery's CEO, who lobbied for the deal, was arrested. (…) It is much better for us in long perspective that Refinery Brod was sold to Russian company than to the British one, as Russia has more oil than the UK, thus oil supplies are guaranteed (personal interview, December 2012).

Direction of Russian foreign direct investments (FDI) in Serbia and Bosnia and Herzegovina revealed that the energy sector was the receiver of the largest amounts of FDI from Russia (Tepavcevic, 2013). Other FDI from Russia in the Western Balkans that followed in the same period included Russian oligarch Oleg Deripaska's company RusAl purchase of the biggest metal plant – Kombinat Aluminijuma Podgorica (KAP) in Montenegro, and Lukoil's purchase of Serbian oil company Beopetrol in 2005. Depending on their socioeconomic impact, they either increased or diminished Russia's political influence in the energy sector: while RusAl's investment in KAP proved unprofitable for the Montenegro's economy, Lukoil made its business with Beopetrol lucrative for both the company and Serbia in general. Additionally, Russian citizens conducted a number of smaller private investments in

tourism and real estate sector in Montenegro and Croatia. While generating profits at the local level, these investments were insignificant in their amounts, and proved politically insignificant.

Russia's Policy towards the Former Yugoslav States during Medvedev's Presidency: The next version of Russia's Foreign Policy Concept was approved in 2008 under the presidency of Dmitri Medvedev and MFA Sergey Lavrov, who was the first post-Soviet Russia's MFA member of a political party, particularly the hard-liner conservative United Russia. While this version of The Concept demonstrates explicitly the multi-vector nature of Russia's foreign policy, discussing mostly the emerging world order, the role of international organizations in that process, and various aspects of security, it refers to the Western Balkans only as a part of Central and Eastern and South and Eastern Europe. Such prioritization demonstrated that the developments in the Balkans, unlike the attempts to oppose NATO in the post-Soviet space, were not in the focus of Russia's foreign policy. On the contrary, the modernization of Russian economy and asserting a revisionist stance for Russia and its role in the multipolar world were among The Concept's top priorities. Another important note in this version of The Concept was "the perspective of loss of the monopoly by traditional West's control over globalization process" (Metcel, 2023). While this version confirms the political proposition concerning Russia's foreign policy interests in general, it does not include the Balkans as any significant region of influence.

The most significant investment by Russian companies in the Balkans in that period, and so far, has been the acquisition of 51% of the shares in the Serbian petrol industry company NIS by Gazprom's daughter company, Gazpromneft in 2008. The start of negotiations regarding this acquisition practically coincided with Kosovo's unilateral declaration of independence in February that year. Russia used its right to veto in the United Nations Security Council to oppose to Kosovo's decision (Tepavcevic, 2018). The fact that Serbia's government sold its largest company to Russian Gazpromneft without tender and at an unreasonably low price was interpreted as a gesture of appreciation for Russia's support for Serbia over the Kosovo issue (Reljic, 2009). In addition to tying up their foreign policies to significant investments, in

2010, Serbia declared its military neutrality. In this way, Serbia remained the only country in the region not seeking NATO membership (Tepavcevic, 2022b). Yet, it did not turn into legislation, as Serbia remains member of NATO's "Partnership for Peace" initiative (Ejdus, 2014). Additionally, Gazpromneft's investment in Serbia also provided Gazprom with an opportunity to control approximately one quarter of Serbia's state budget, making it along with the building of the South Stream gas pipeline – Russia's major political leverage in the Balkans (Reljic, 2009; Tepavcevic, 2018). Simultaneously, this Russian company's investment softened the unavoidable negative impacts of the global financial crisis of 2008–2009 on Serbia's economy (Tepavcevic, 2022b). All these involvements of Russia in the former Yugoslav republics became possible, firstly, because the former Yugoslav business community in Russia attracted investments from Russia to post-Yugoslav republics, and; secondly, because of the virtual absence of the competition in acquisitions and relatively low acquisition costs in Bosnia and Herzegovina, Serbia, and Montenegro (Tepavcevic, 2022b).

These activities of the Russian companies in the Western Balkans were paralleled with turmoil across the former Soviet territories: Russia's armed forces conducted a five-day long military action preventing Georgia's government attempt to regain control over its breakaway regions Abkhazia and South Ossetia. The results of this operation were two-fold. First, it led to long-term presence of the Russian troops on 20% of the internationally recognized territory of Georgia. Second, it left many Georgians internally displaced, and consequently, the majority of Georgians with bitter attitudes towards Russia.

Annexation of Crimea and Russia's relations with the Western Balkans

The next version of Russia's Foreign Policy Concept was approved in 2013, after Vladimir Putin's return to Kremlin as a president. Following similar postulates as the two previous versions, 2013 Concept highlighted the weakening of the influence of the most economically advanced countries because of the global economic crisis. Vaguely referring to the Western Balkans as the region where international organizations failed to prevent wars, this version of The Concept was the

first to recognize the emergence of Asian-Pacific region as a center of power and development. In addition, exactly this version of The Concept sought mentioning the inclusion of Ukraine into the CIS integration processes. Therefore, this version of The Concept reflects certain expansionist aspirations for the first time in Russia's post-Soviet foreign policy, confirming the political proposition concerning particularly post-Soviet space.

This version of The Concept was reflecting business interests of Russia's political elites and their partners in Ukraine mostly represented by then Ukrainian President Viktor Yanukovich and his Party of Regions, an influential political force of businesspersons from then Russia-leaning Eastern Ukraine. In February 2014, followed by Yanukovich's rejection to sign an Association Agreement between the EU and Ukraine and consequential Euromaidan protests, Yanukovich's government was ousted in the aftermath of Euromaidan protests in Ukraine (Tepavcevic, 2024). Soon after, in the end of February 2014, Russian military occupied Autonomous Republic of Crimea, and in March 2014, Russia's government annexed the peninsula from Ukraine, severely violating international law. Russia's actions did not represent an immediate "a stratagem of geopolitical expansion", nor did they pose immediate implications for the global balance of power (Saluchev, 2014). However, Crimea's annexation nurtured the violent conflict in Eastern Ukraine, which resulted in 54.000 deaths between April 2014 and January 2022 (United Nations Human Rights Office of the High Commissioner, 2022). Indeed, although it did not cause violent conflict inside Crimea, Russia's actions in the peninsula shaped the nature of Russia's influence in the post-Yugoslav republics. As Bechev (2023) correctly noted, the Russian approach has been unashamedly opportunistic, often at Serbia's expense. Moscow has selectively invoked a Kosovo precedent to justify its own actions, recognizing as independent states Georgia's breakaway territories of South Ossetia and Abkhazia in August 2008 and the so-called people's republics in Ukraine's Donbas region in February 2022.

However, it visibly sharpened the ideological dispute between far-right nationalists and liberals in Serbia: the former supported the annexation relating it to the hope to return Kosovo under Serbia's control with the help of Russia. On the contrary, center-right and liberal political forces in Serbia perceived Russia's annexation of Crimea as another

violation of international law, which decreased Russia's influence in the UN over Kosovo's status, and consequently, Serbia's positions on the issue.

Migration Crisis

Russia's Foreign Policy Concept 2016 version was developed and approved in the international context in which Russia's annexation of Crimea had already happened as well as Western sanctions were implemented, but they were limited to Russian companies and individuals, who directly participated in the annexation. In contrast to all previous versions, this version of The Concept demonstrated an open declaration of Russia as one of the regional centers of power in a multipolar world, and opposition to the US domination in the global politics, which was provoked by the geopolitical expansion of the US, EU, and NATO. In addition, The Concept of 2016 noted the resolution of the conflicts in Syria and in Ukraine as top regional priorities. This prioritization demonstrates the major shift in Russia's foreign policy regional interests away from Europe towards Asia, and open readiness to counterweight the Western institutions' influences even by military means, confirming the proposition concerning Russia's assertiveness in pursuing geopolitical interests.

These events overlapped with European migration crisis, which led to Brexit, and consequential post-Brexit fatigue within the EU. According to Lažetić (2018), for Serbian nationalists, this migration crisis reinforced victimhood narratives about Serb refugees from Bosnia, Croatia and Kosovo, who had been "expelled from their homes by ethnic enemies" and consequential resentment against NATO due to bombing Serbia in 1999, and against the West for supporting Kosovo's Albanians. In turn, during the migration crisis that refocused the Serbian far-right nationalists from Serbia's neighbors as ethnic enemies to the refugees from the Middle East and Asia, which was seen partially as the result of Russian nationalists ideological influence (Krasteva, 2021). While such shift brought Serbian nationalists closer to the European far right, it also made Serbia, as Lažetić (2018) pointed out, into a "conference room' where Russian and European far right activists connect and strategize together." For instance, Lažetić (2018) stated that "Russian far-right

ideologue Alexander Dugin, author of the Fourth Political Theory is often seen in Serbia with Jim Dowson, founder of Britain First, and the former British National Party leader Nick Griffin, who have been "exiled" from Europe."

Russia's Influence in the former Yugoslavia during COVID-19 Pandemic

Due to simultaneous lockdowns in nearly all parts of the globe, the COVID-19 pandemic was an unprecedented global crisis, during which the specificity of the virus and the absence of the relevant vaccine made these lockdowns lasting. It took months to vaccines developed in China, where the virus was recognized, to be certified in Europe. Almost parallel to their Chinese colleagues, Russian specialists developed anti-COVID vaccines. However, due to the company producer's refusals and delays in providing standard requirements for the drug approval process (Reuters, 2021), Russian anti-COVID vaccines have never passed the World Health Organization's (WHO) certification. Nevertheless, Russian Sputnik-V was the first to supply the Western Balkans, and the Russian political leadership applied its strategy of political influence through energy supplies on the vaccine supplies.

Russia's "vaccine diplomacy" in the Balkans had double effect. First, Russia provided Serbia with Sputnik-V early in the 2021, when most of the EU member states lacked supplies of any anti-COVID-19 vaccines. Second, consequently, the availability of anti-COVID-19 vaccines in Serbia prompted vaccine tourism from all countries of the region to Serbia for receiving otherwise unavailable anti-COVID vaccine (MUNI, 2023). In short-run this increased Serbia's positive image in the region, where in the mainstream political discourses it has usually been portrayed negatively because of its, as previously discussed, relative power stance vis-à-vis most countries in the region (Tepavcevic, 2022b).

Effects of Russia's Invasion of Ukraine on Its' Influence in the post-Yugoslav space

The beginning of 2022 was also marked in the former Yugoslav countries by several striking events. First, as one of the rare remaining European capitals where Russian citizens can travel without visas,

Belgrade hosted the informal meeting of the Russian political opposition. This informal meeting would probably remain unnoted if the Interior Minister of Serbia, Aleksandar Vulin had not initiated to report to the Kremlin about the details of this meeting. Such demonstration of loyalty revealed the high level of Putin's regime influence in Serbia prior to February 24, 2022.

Second, parallel to this Vulin's unilateral move, the long-standing political leader of Serbs' Republic, Milorad Dodik announced his intention to declare this entity independent from the rest of Bosnia and Herzegovina. His assertiveness was underpinned by long-standing political rhetoric and Zarubezhneft's investment-prompted economic support by Russia, and with some right-wing political forces within the EU, particularly in Hungary and Croatia. This renewed the old image of post-Yugoslav region as the one with the high potential for the violent conflicts. Overall, in the beginning of February 2022, the integration of the rest of the post-Yugoslav Balkans into the EU seemed as far as ever before.

However, Russia's full-fledged war on Ukraine that started on February 24, 2022 radically changed the prospects of Russia's influence in the Balkans. For the EU, the beginning of a full-scaled operation in Ukraine turned into the most pessimistic scenario concerning migration and energy crises. Simultaneously, for the former Yugoslav non-EU states, where the tensions, as discussed above, have persisted with changeable intensity over the last three decades, Russia's full-scale military invasion of Ukraine meant much more than migration and energy crises. The statements of political leaderships of these countries revealed fears and desperation. The Prime Minister of Croatia, Andrej Plenkovic called the invasion "the catastrophe for the whole Europe" (IndexHR, 2022). On February 24th 2022, the President of Serbia, Aleksandar Vucic spent the whole day, unsuccessfully trying to formulate a clear position about the attack. He made an official statement in the evening, saying that it is the biggest tragedy for Serbia to see two fraternal Slavic countries in war with each other (Tepavcevic, 2022b). Similarly, the EU officials noted that Serbia's closeness to Russia may hinder Serbia's further EU integration (Politico, 2023). Their understanding of the sharp twist in the role that Russia has played for these countries since Yugoslavia's breakup was behind these statements,

and consequences became visible soon after the beginning of the invasion. These reactions demonstrate the correctness of Rasidagic and Selo-Sabic (2013) argument that "Small states have a few policy options to choose from in foreign affairs realm. One of them is building a strategic partnership with a big power. There is nothing unethical or unusual in such asymmetric power-relationship."

Over seven million people from Ukraine (UNHCR, 2022) and between three and five million from Russia left their homes (ERR, 2022), the former running from the bombs, the latter running from increased danger from political and ideological prosecutions, economic uncertainty, and more recently – from mobilization. About 150.000 of Russian de-facto refugees in Serbia since 2022 (Euronews, 2024) has not fit into the dominant mostly far-right-related narrative of Russia as a defender. Quite the contrary, majority of Russian refugees in Serbia have been fierce opponents of Putin's regime as their relocation also witnesses.

It was quite easy decision to come to Serbia: visa is not required to enter, the language is similar to Russian, so it is easy to learn, and the climate is pleasant. (…) Though many people came here from Russia as employees relocators, in fact they run from the Putin's repressions and mobilization. I am factually Russian refugee in Serbia as many others, and I learn the language and I try to assimilate to stay here. I do not see any perspectives in Russia in any near future (online communication, March 2023).

In addition to multinational companies' employers' relocation, many small and medium businesses from Russia moved to Serbia. By June 2023 up to 4.500 firms were registered in Serbia by the Russian citizens, while – for the comparison – for the same period in Hungary only 30 firms were established by the Russian citizens, despite some investments favorable state programs (Szabo, 2023). Therefore, after thirty years of being the major host country for the refugees from the region, in the early 2020s, Serbia appears again as the major receiving country in the Balkans, this time (though paradoxically) for the refugees from Russia, whose number is estimated to about 200.000 (Politika.rs, 2023) – the size of population of Serbia's third largest city, Novi Sad. This influx of Russians with the political views fiercely opposing the Putin's regime could in some mid-term influence Serbia's foreign policy at least towards Putin's regime, but also and towards further EU integration.

Finally, the newest version of The Concept was approved at the time of writing of this article, in May 2023. The document reflects on the revolutionary changes humanity is currently encountering alluding to the war in Ukraine, which, as The Concept claims, will result in "a more equitable multipolar world order". These changes are described as being inevitable and only opposed by Western countries, which would try to prevent these shifts of power. The document's main thematic focus is on a deepening "crisis of economic globalization", which envisions intensification of "the fragmentation of the global economy". The Concept suggests that Russia's foreign policy regional focus shifts towards Asia and announces the aspiration to control the 'near abroad', i.e. the post-Soviet space, leaving the Balkans practically outside its' zone of interest.

Table 2. Major postulates of Russia's Foreign Policy Concept since 1991 (Source: author's view based on literature review)

Russia's Foreign Policy Concept about the Balkans	**Year of Issuing Foreign Policy Concept**
The Balkans are not mentioned in the Concept separately; post-socialist Europe is noted as the region of transformation and search of identity	First post-Soviet Russia's Foreign Policy Concept -1992
Third regional priority and mention of FRY and its' territorial integrity as significant factor in the Balkans	Second post-Soviet Russia's Foreign Policy Concept – 2000
Third regional priority, but only in the context of Central and South Eastern Europe	Third Russia's Foreign Policy Concept – 2008
Vague shift of interest towards Asia-Pacific region, and remaining interest in the CIS	Fourth Russia's Foreign Policy Concept – 2013
Open opposition to the West as the major center of global power, and regional prioritization of CIS and Asia	Fifth Russia's Foreign Policy Concept – 2016
Shift towards Asia and open aspiration to control the post-Soviet space	Sixth Russia's Foreign Policy Concept – 2023

Conclusions

In conclusion, the analysis has demonstrated that all propositions from scholarly discussions about Russia's influence in the post-socialist Europe were applicable to the republics of former Yugoslavia, though they varied across Yugoslavia's successor states and periods. By overall playing the role of counter-balancer of the Western influence (Tepavcevic, 2022b), Russia's influence in the post-Yugoslav Balkans allows to paraphrase Neumann (1998) argument that Russia means different power in different periods, and in different contexts during the same period.

Indeed, as the analysis above suggests, Russia's influence in the post-Yugoslav Balkans over the last three decades gradually shifted between two opposites. Starting from the weak power contributing to ending the conflicts of Yugoslavia's dissolution and peace resolutions in the 1990s, Russia's influence in former Yugoslavia throughout 2000s and 2010s represented an international factor of economic stabilization. Russia's influence in post-Yugoslav Balkans since 2014 has been a one of a distant international power contributing to the potential destabilization of the region. At the same time, Russia's full-scaled invasion of Ukraine decreased Russia's political influence in the Western Balkans. Finally, the invasion accelerated the long-stalled region's EU integration: in December 2022, Bosnia and Herzegovina was finally granted the EU candidate status for which it waited since 2016. Simultaneously, despite being still unrecognized as an independent state by some of most significant EU member states, Kosovo applied for the EU candidate status just days after. Last but equally important, further acceleration of the region's EU integration will be the key prevent new escalations of previous conflicts in the region and to confirm the EU status both as a major power and a stabilizer. If this highly demanding task proves successful, further liberalization in the post-Soviet countries will appear as the spillover effect.

References:

1. Abdelal, R. (2005). *National Purpose in the World Economy*, Cornell University Press.

2. Bechev, D. (2023). *Hedging Its Bets: Serbia between Russia and the EU.* Carnegie Endowment Europe.

3. Bilten, G., (1991). *Ethnic composition of Bosnia-Herzegovina population.* Sarajevo: Zavod za statistiku Bosne i Hercegovine.

4. Bosnia and Herzegovina Government. (2018 – 2023). *Foreign Policy Strategy of Bosnia and Herzegovina [Online]*. Available: https://dijaspora.mhrr.gov.ba/wp-content/uploads/2018/06/Strategija-vanjske-politike-Predsjednistva-BiH.pdf.

5. Paravac, B. (2003). *Basic directions and activities of BiH foreign policy [Online].* Embassy of Bosnia and Herzegovina Brussels. Available: https://www.bhembassy.be/foreign_policy.html [Accessed July 5, 2023 2023].

6. Croatia's Ministry of European And Foreign Affairs. (2023). *Commemorating Croatia's 10th EU membership anniversary [Online].* Available: https://mvep.gov.hr/press-22794/commemorating-croatia-s-10th-eu-membership-anniversary/257534.

7. Donaldson, R. & Nogee, J. (20050. *The Foreign Policy of Russia: Changing Systems*, Enduring Interests, Routledge.

8. Ejdus, F. (2014). "Serbia's Military Neutrality: Origins, effects and challenges." *Croatian International Relations Review*, 20, 43-71.

9. Err, E. (2022). *S nachala voiny rossijane vhezzhayut v evrosojuz v osnovom cherez finljaniju i estoniju [Online*]. Estonia.

10. Euronews. (2024). *The plight and hope of Ukrainian and Russian refugees in Serbia.*

11. *Indexhr 2022. Reakcije na ruski napad na Ukrajinu*: "Ovo je katastrofa za Europu".

12. Kovacevic-Bielicki, D. (20170. *Born in Yugoslavia- Raised in Norway: Former Child Refugees and Belonging*, Oslo, Novus Press.

13. Krasteva, A. (2021). *Balkan Migration Crises and Beyond. Southeastern Europe,* 2021, 173-203

14. Lažetić, M. (2018). 'Migration Crisis' and the Far-Right Networks in Europe: A Case Study of Serbia. *Journal of Regional Security* 13, 131-178.

15. Metcel, M. (20230. *Kak menyalas' Kontseptsiya vnyeshnyei politiki Rossii*.

16. Ministry of Foreign Affair of the Russian Federation. (1992). "Kontseptsiya vnyeshnyei politiki Rossiyskoy Federatstii." *Russia matters*.

17. Montenegro's Ministry of Foreign Affairs. (2023). *Bilateral cooperation* [Online]. Available: https://www.gov.me/en/article/bilateral-cooperation.

18. Muni, T. (2023). "Dušan Mladenović: Free vaccination for citizens of Serbia and neighboring countries mitigates pandemic's impact on tourism." In: Sosnova, J. (ed.). *Masaryk University Faculty of Economics and Administration*.

19. Neumann, I. (1998). "Russia as Europe's other." *Journal of Area Studies* 26–73.

20. Nygren, B. (2007). *The Rebuilding of Greater Russia Putin's Foreign Policy Towards the CIS Countries*, Routledge.

21. Orban, A. (2008). *Power, Energy, and the New Russian Imperialism*, Westport, Connecticut & London, Praeger Security International.

22. Politico, P., W. (2023). *Serbia 'not enthusiastic' about EU membership anymore, says president.*

23. Politika.Rs. (20230. "Ноје цирхер цајтунг: најезда руских досељеника на Београд."

24. Rasidagic, E. (20130. "Involved by default: external actors and foreign policy of the Western Balkan States." *CEU Political Science Journal* 8, 348+.

25. Rasidagic, E. & Selo-Sabic, S. (2013). "Foreign Policy Traps: Small States and Big Powers in the Western Balkans." In: Nikolic, M., ed. Strategic Paths of *Development and Position of Serbia in Contemporary International Relations*, April 22, 2013, Belgrade, Serbia.

26. Reljic, D. (2009). *Rusija i zapadni Balkan*, ISAC Foundation.

27. Reuters. (2021). *Exclusive European efforts to assess Russia's Sputnik V vaccine stymied by data gaps*. In: Rose, M., Ivanova, P., Parodi, E. (ed.). *Reuters*.

28. Saluchev, S. (2014). "Annexation of Crimea: Causes, Analysis and Global Implications." *Global Societies Journal*, 2, 37-46.

29. Serbia's Ministry of Foreign Affairs. (2021). *Bilateral relations Serbia - Russian Federation* [Online]. Available: https://www.mfa.gov.rs/en/foreign-policy/bilateral-cooperation/russia.

30. Serbia's Ministry of Foreign Affairs. (2022). *EU Integration* [Online]. Available: https://www.mfa.gov.rs/en/foreign-policy/eu-integration/political-relations-between-serbia-and-eu.

31. Stent, A. (2008). "Restoration and Revolution in Putin's Foreign Policy." *Europe-Asia Studies*, 60, 1089-1106.

32. Szabo, D. (2023). *Úgy ajánlják az oroszoknak a magyarországi letelepedést, mintha állami program lenne rá*. Portfolio.hu.

33. Tepavcevic, S. (2013). *Russian Foreign Policy and Outward Foreign Direct Investments: Cooperation, Subordination, or Disengagement*? Ph.D. Dissertation [Online]. Budapest: Central European University.

34. Tepavcevic, S. (2015). *The motives of Russian state-owned companies for outward foreign direct investment and its impact on state company cooperation: observations concerning the energy sector.* Transnational Corporations, 23, 29-58.

35. Tepavcevic, S. (2018). "In the Bear's Shadow? Russia's International Image and Its Influence on Investments of Russian Companies in Post-Socialist Europe." *Journal of East-West Business*, 24, 108-137.

36. Tepavcevic, S. (2021a). "Changing Geography, Retaining the Mentality: Social and Economic Integration of Post-Soviet Immigrants in Austria and Hungary." *Review of Economic Theory and Policy*, 3, 137-154.

37. Tepavcevic, S. (2022b). "The End of the 'Sanitary Zone'? The Conflict in Ukraine and its' Impact on Russia's Influence in the Balkans." *Visegrad Europe Central European Journal,* XV, 23-30.

38. Tepavcevic, S. (2024). Global Crises, Resilience, and Future Challenges: Experiences of Post-Yugoslav and Post-Soviet Migrants, Stuttgart, Ibidem Press.

39. Tsygankov, A. (20060. "If not by tanks, then by banks? The role of soft power in Putin's foreign policy." *Europe-Asia Studies*, 58, 1079-1099.

40. United Nations Human Rights Office of the High Commissioner, 2022. Conflict-related civilian causalties in Ukraine. January 27, 2022.

41. United Nations Human Rights Office of the High Commissioner, 2022, Operational Data Portal - Ukraine Refugee Situation [Online].

42. Yesson, E. 2000. *NATO and Russia in Kosovo*. https://www.jstor.org/stable/23615938#metadata_info_tab_contents.

OPEN SOURCE INTELLIGENCE

WHAT IS REALLY "OPEN SOURCE INTELLIGENCE"? A CONCEPTUAL ANALYSIS OF THE DIFFERENT NOTIONS OF OSINT

Ainara BORDES PEREZ*

Abstract:

The recent Ukrainian conflict has spurred innovative uses of Open Source Intelligence (OSINT) and nurtured several academic articles on the topic. It is just the last example of an overall rapid evolution of OSINT since the emergence of the Internet in the '90s, the arrival of smartphones, and the flourishing of social media and other openly available sources online in the early 21st century.

This fast evolvement has encouraged researchers and practitioners to study the validity, significance and legitimacy of this type of intelligence (OSINT) coming from openly accessible sources. However, in spite of the increased use and investigation of OSINT, its rapid evolution has hindered any universal definition of it. While practitioners and scholars have tried to conceptualise it since the beginning of its institutionalisation, different definitions shaped over the course of OSINT's expansion are ambiguous at times, vague, or incomplete. The latter has an impact on the creation of procedures for practitioners, recruitment needs, development of regulations and research.

This article studies those nuances in terminology and extracts the main conceptual differences present in some of the most prominent definitions offered by practitioners, oversight bodies and academics on OSINT. It does so through a comparative analysis of the definitions presented, which are not limited to one jurisdiction or body. Offering a structured taxonomy of the different shades of OSINT is the novelty of this article, which is a necessary first step towards a potential universal definition of the term.

Keywords *Open Source Intelligence, OSINT, definitions, conceptual nuances, Intelligence Services, Law Enforcement*

Introduction

Open source intelligence (OSINT) as a concept has rapidly evolved in the last decades. While open source information has supported

* A dual Ph.D. candidate at "Mihai-Viteazul" National Intelligence Academy & University of Malta, email: ainara.bordes.17@um.edu.mt.

governmental decisions since the beginning of intelligence (Schaurer & Störger, 2013), OSINT as a concept was first coined during the Cold War in the '60s and it was not until the '90s that, due to the emergence of the Internet, it started to be mentioned more regularly in publications due to the emergence of the Internet (Hatfield, 2023, pp. 6-7). Until then, monitoring and translating media was the main part of OSINT practices (Pallaris, 2008).

Advances in information technology at the end of the 20th and beginning of the 21st century with the wide spread of the Internet, the arrival of smartphones and the creation of social media, enabled new open sources to flourish and multiply, exponentially boosting the amount of openly available data. These, coupled with the opening of democracies, several geo-political changes, and some intelligence *failures* – expression used by Chris Pallaris (2008) – at the beginning of the 21st century (US 9/11, Madrid 2004, London 2005), pushed the intelligence community (IC) and law enforcement authorities (LEAs) towards stronger OSINT capabilities, and a feeling of urgency spurred its use (Hatfield, 2023, pp. 10–11). The latter, and advanced developments in data-mining and analytic software,[1] both in public and private sectors, shaped and re-shaped the notion of OSINT in the last couple of decades. The conflict in Ukraine and the various innovative ways of OSINT exploitation within it are the last examples of its changing nature (Freear, 2023).

This fast evolution has hindered any universal definition of OSINT. Practitioners and scholars have tried to conceptualise it since the beginning of its institutionalisation. However, different definitions shaped over the course of OSINT's evolution can be considered ambiguous, vague or incomplete (Wells & Gibson, 2017, p. 86).

The importance of defining any intelligence discipline (INT)[2] is diverse. From an operational perspective, prioritisation of collection efforts often follows the classification of intelligence disciplines. When collected data or information are later analysed by all-source analysts, credibility and validity are also often evaluated in accordance with the requirements per intelligence discipline (Williams & Blum, 2018, p. 21).

[1] For the purposes of this study, "data-mining software" or "data mining tools" encompasses all tools used to collect, extract and analyse large amounts of data.
[2] Whether OSINT is or should be an intelligence discipline will be discussed below.

In terms of recruitment purposes, hiring and organizing data scientists involves understanding the expertise and needs required for each intelligence discipline. Having a vague or ambiguous concept of OSINT does not help in drafting a job description, nor in assessing appropriate candidates for it (Hatfield, 2023, p. 6; Williams & Blum, 2018, p. 53). Also, from a legal perspective, intelligence practices are assessed according to their impacts on human rights (specified in international and national regulation) and in accordance with other applicable laws. These laws are usually later granulated by sectorial policies, guidance and procedures, which can sometimes be internal and classified by the institution.[3] Where OSINT as a concept is ambiguous, regulation and subsequent internal policies may become disparate regarding its feasible uses and regulatory and oversight needs. As a consequence, OSINT practices may have different legal and procedural protection in diverse security and intelligence services (SISs) and LEAs, despite prompting similar impacts on human rights and society as a whole (Omand et al., 2012, p. 820; Rønn & Søe, 2019, p. 11). Lastly, the interest in defining intelligence disciplines is also relevant for research purposes. Currently, studying the various endeavours related to OSINT requires defining the material scope of the concept by the researcher. Due to a lack of a universal definition of OSINT, published material might cover different activities, which makes it difficult to advance in this research area smoothly. Having an accepted international definition of OSINT would facilitate the study of this topic from all potential angles.

This article aims to illustrate, describe and analyse the different conceptualisations, descriptions, and opinions of the notion of OSINT, offered by the most prominent academics and practitioners on the topic throughout its evolution. For this, the study adopts a qualitative research method of a comparative nature, where it first exposes existing definitions of OSINT through a literature review of academic articles, institutional reports and policies, and studies their differences thereafter. Whilst most of the definitions may share similar characteristics, there are several disparities among them, some characteristics appear only

[3] See for example the UK National Police Chief's Council's (NPCC) Guidance on Open Source Investigation/Research (National Police Chief Council, 2015).

in some of the definitions, and many of the features need further understanding. Addressing the lack of a universal definition and structuring the differences in concept is the novelty of this article. Tackling and exposing those differences is the first step towards a debate around a potentially commonly accepted notion of OSINT.

Bearing this in mind, the article starts with a sequence of well-known OSINT definitions proposed by practitioners, scholars and policy-makers. It continues with the analysis of those definitions, divided into six different sections where the notion of OSINT is or can be interpreted differently in accordance with the definitions exposed. The study finalises with a section on conclusions on the differences encountered.

Defining Open Source Intelligence

Practitioners, scholars and policy-makers have tried to define Open Source Intelligence since the beginning of its institutionalisation in the '60s, until today. The following section encompasses a non-exhaustive list of the most prominent definitions of OSINT proposed by experts in the field over the years. These definitions are the benchmark for a later analysis of the similarities, divergences and unknowns of the notion of Open Source Intelligence.

Starting from the perception of OSINT by experts in the United States (US), the OSS Academy, a corporation founded by Robert David Steele to promote the understanding and opportunities of the use of OSINT, offered the following definition in 1998: "OSINT results from the integration of legally and ethically available multilingual and multimedia sources, with the heretofore largely secret processes of national intelligence: requirements analysis, collection management, source validation, multi-source fusion, and compelling presentation." (R. Steele & Lowenthal, 1998)

In parallel, Joseph Nye, Head of the National Intelligence Council in the US between 1993 and 1994, stated that "Open source intelligence provides the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle. But they are not sufficient of themselves. The precious inner pieces of the puzzle, often the most expensive to obtain, come from traditional intelligence disciplines. Open source intelligence is the critical foundation of the all-source intelligence

product, but it cannot ever replace the totality of the all-source effort." (Sands, 2005)

A decade later, the United States Congress adopted the Defence Authorization Act for Fiscal Year 2006, which considered that "Open Source Intelligence [is] produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." (National Defence Authorization Act for Fiscal Year 2006 - Intelligence Community Directive Number 301, n. d.)

The Central Intelligence Agency (CIA) stated in 2010 that "information does not have to be secret to be valuable [and conceptualised open source intelligence as the] information that can be gathered from open sources, including the Internet, traditional mass media (newspapers, TV, radio broadcasts), specialized journals, conference proceedings, think tank studies, photos, maps and commercial imagery products." (Central Intelligence Agency, 2010)

Some years later, in 2018, the RAND Corporation[4] introduced the dilemma of the rapid evolution of technology and the creation of new online open sources into their definition (Williams & Blum, 2018, p. 9). While the high-level conceptualisation of OSINT proposed by them remained plain and generic – "we define OSINT as publicly available information that has been discovered, determined to be of intelligence value, and disseminated by a member of the IC," they acknowledged a lack of universal notion for OSINT and the difficulties for it due to the rapid evolution of the Internet and technology overall. With this in mind, they worked on a new taxonomy of current types of open-source information (OSINF) and data mining methods to create the notion of a "second generation of OSINT". According to them, open sources should be classified between institutionally generated content (news media and grey literature) and individually driven online content (long-form social media content such as blogs, and short-form social media content such as Facebook and Twitter content with little intelligence value individually). Moreover, they also described existing open-source analytic methods (i.e., lexical analysis, social network analysis, geospatial analysis) as part of the characterisation of the second-generation OSINT. Finally, they

[4] A widely US-based respected nonpartisan and nonprofit research organisation that aims at developing solutions to public policy challenges through research and analysis.

suggested a near-future emergence of a "third generation of OSINT", where evolution to Web 3.0 would include direct and indirect machine processing of data, machine learning and automated reasoning (Williams & Blum, 2018, p. 39). Figure 1 below shows the characteristics of the proposed OSINT generations by RAND Corporation:

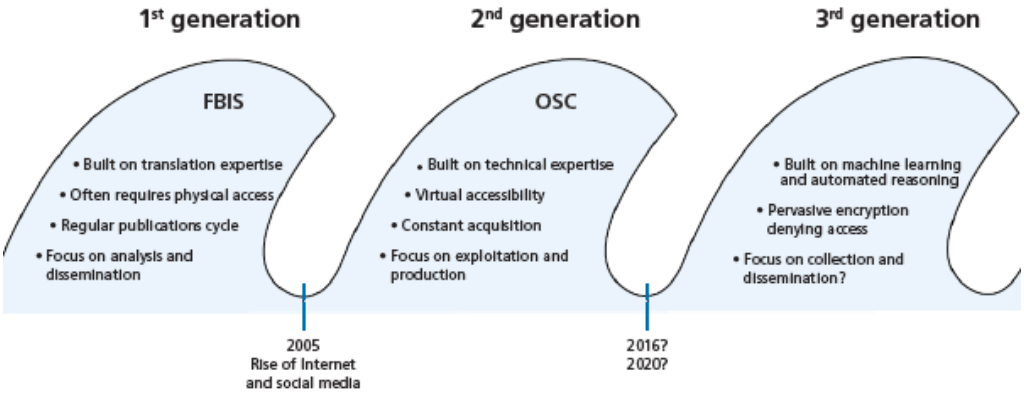


Figure 1: Characteristics of OSINT generations by RAND Corporation (Williams & Blum, 2018, p. 40)

To conclude, the last US-based definition of OSINT exposed in this article is the one provided this year (2023) by Joseph M. Hatfield, a US Naval Intelligence Officer and Assistant Professor at the US Naval Academy. As he explicitly exposes in the title of his article "There is no such thing as Open Source Intelligence", he argues that OSINT "is a fundamentally incoherent concept that should be abandoned" (Hatfield, 2023, p. 1). He challenges the underlying criteria used to demarcate OSINT as a stand-alone INT and considers that it had had its validity to help scholars and practitioners appreciate the new unclassified information that emerged with the creation of the Internet in the '90s, but this value no longer exists. He considers the term should be discarded altogether, and that openly derived sources of information should be reclassified within traditional INTs (Hatfield, 2023).

If we move to the European landscape, diverse voices have also tried to conceptualise Open Source Intelligence over the years. One of the examples is the Ministry of Defence in the UK, which defined OSINT

in 2011 as "intelligence derived from publicly available information, as well as other unclassified information that has limited distribution or access." (Ministry of Defence (UK), 2011, p. 12)

The National Police Chiefs Council (NPCC) Guidance on Open Source Investigation/Research in the UK provided a more extensive and specific definition in 2015 where they mentioned that "[Open Source Research is the] collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise to use as intelligence or evidence … ." (National Police Chief Council, 2015).

Switching to a more recent definition, the German think tank Stiftung Neue Verantwortung analysed the notions and practices related to commercial and publicly available data within the different European intelligence agencies. According to this think tank, "OSINT comprises openly accessible data from sources such as the media, social media, and other public data" (Wetzling & Dietrich, 2022). The report also offers a non-exhaustive summary of non-legally compelled intelligence services' access to personal data, where voluntary submissions of data by the private sector, commercially available data, and OSINT are included (see Figure 2 below).

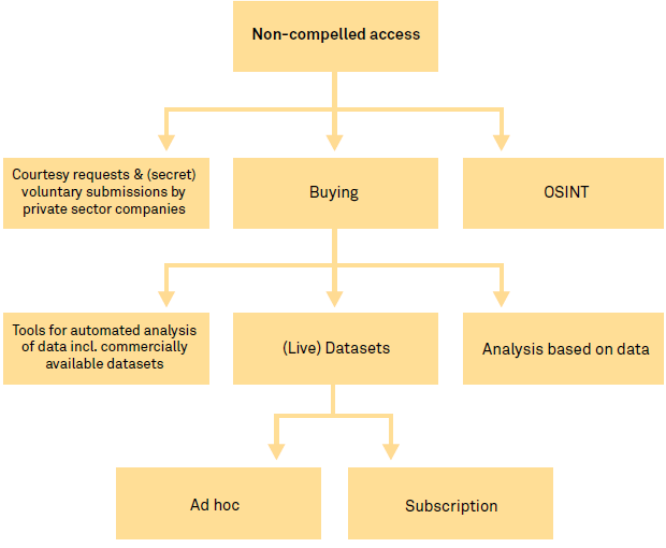


Figure 2: Modes of non-legally compelled access to data by SISs (Wetzling & Dietrich, 2022)

According to this report, the three non-compelled access modes can be understood as OSINT practices in some national regulations. The report emphasises the ambiguous terminology surrounding OSINT within SIS legislation (Wetzling & Dietrich, 2022, p. 34).

Finally, the last definition analysed is the one offered by Arno Reuser[5] in 2018, who mentioned that "Open Source Intelligence is a collaborative, integrated methodology and production process where customers' intelligence requirements are met by providing them with actionable intelligence that is produced through a process of synthesis and analysis based on a representative selection of open source information that is validated, reliable, timely, and accurate". According to this notion "… Open Source information or open sources, is all information in any format that can be acquired by anyone without any restrictions, whether for free or commercial, in a legal and ethically acceptable way" (Reuser, 2018). This notion takes relevance in today's uses of OSINT within the conflict of Ukraine as it is explained below.

Whilst most of the definitions share similar characteristics, (1) there are several disparities among them, (2) some characteristics appear only in some of the definitions, and (3) many of the features need further understanding. For example, is OSINT "information that can be gathered from open sources", as the CIA's definition states, or is it instead an "intelligence product"? Can OSINT be a stand-alone intelligence product as Arno Reuser, the NCPP and the US Congress suggest, is it just the foundation for other intelligence products, as the OSS Academy and Joseph Nye propose, or is it a concept that should disappear as Hatfield suggests? At the same time, some of the OSINT characteristics need further explanation: What is the meaning of *open sources* and where are the boundaries? What does "openly available information" mean? And finally, is OSINT open (overt) intelligence or does the openness refer only to the sources? The following sections attempt to answer those questions.

[5] Founder of the Open Source Intelligence Unit at the Dutch Defence Intelligence and Security Service (DISS) and founder of Reuser's Information Services in the Netherlands.

OSINT: Data, information, or intelligence?

The difference between data, information and intelligence is a basic one for all INTs, however, some of the different definitions exposed above seem to use these three terms interchangeably when defining OSINT.

Looking at the CIA's definition, OSINT is conceptualised as *information* that can be gathered from open sources. *Intelligence* and *information* are, nevertheless, two terms that cannot be equated. OSINT is indeed generally considered the output or the *intelligence product* derived from the processing of data and information that are accessible in open sources.[6] In other words, open source data (OSD) and open source information (OSINF) are the raw material for the creation of OSINT. NATO's Open Source Intelligence Handbook (NATO, 2001) offers a good explanation of these concepts, delimiting the notions of OSD and OSINF from OSINT, and describing the notion of *validated-OSINT*.

OSD consists of openly accessible raw material that has not been processed or edited. These primary data may comprise a photograph, a commercial satellite image, a debriefing of a government official, or technical data such as meta-data. When raw data are put together, analysed, edited, filtered and validated up to a certain level – in accordance with the requirements or needs at each moment, they become OSINF.

Likewise, open sources can also contain published OSINF that has already gone through editing and analysis and offers a clear understanding of a situation or a phenomenon. Usually, OSINF material is available from sources that have wider and easier distribution mechanisms. These sources can be traditional media, academic journals or government reports (Minas, 2010, pp. 8–11; NATO, 2001, pp. 2-3). OSINF material has received a variety of names over the years, such as: *non-secret information, overt information, unclassified information, and public information*. Likewise, the words *information* and *intelligence* have sometimes been used interchangeably, and terms like *overt intelligence* and *white intelligence* have inaccurately been employed to name both OSINF and OSINT (Saunders, 2000, pp. 12-13).

[6] The term 'open sources' is analysed in the following section.

Whilst OSINF is already a refined product providing a comprehensible story, it cannot be considered OSINT yet. OSINT is created when different OSINF and OSD materials are carefully selected, analysed, filtered, and validated, creating a compressed assessment that addresses a specific question, at a specific time, for a specific user. When OSD and OSINF materials, together with the OSINT product are analysed in terms of credibility, relevance and utility, the final product can be named *validated-OSINT* (Minas, 2010, pp. 8–11).

Thus, to summarise, OSINT does not equal *information*. It is instead an intelligence product or assessment that addresses a specific requirement of a user, on a specific topic and timing, through the processing of OSINF and OSD.

***Open sources*: what does it mean?**

The concept of *open sources* is one of the pillars of OSINT, and most of the definitions provided emphasise this. However, none of these definitions details its meaning *per se*. For instance, Arno Reuser equates *open source information* with *open sources*. However, these two terms may not represent the same thing. *Information* usually refers to the content that is found on a supporting platform, which is "the source". While the two terms are interconnected, the concepts differ.

As an alternative, the CIA, while it does not strictly define *open sources*, offers a list of sources that can be considered as *open sources*. More specifically, it conceptualises OSINT as the "information that can be gathered from open sources, including the Internet, traditional mass media (newspapers, TV, radio broadcasts), specialized journals, conference proceedings, think tank studies, photos, maps and commercial imagery product." (Central Intelligence Agency, 2010)

The CIA's definition provides an interesting point to analyse regarding the dynamism of the sources. To begin with, it offers a first glimpse of the main open sources available today, while it emphasises the dynamism of those sources with the use of the word *including*, which leaves an open door to other sources to be included in the list. Indeed, the NATO Open Source Intelligence Handbook (NATO, 2001) adds a few more sources to the CIA's list: commercial online databases (according to the Handbook, stand-alone sources separated from the Internet),

overt human experts (i.e. journalists)[7] and grey literature. The latter is a sub-group of open sources that needs special requirements, such as physical attendance or specific timing to acquire the information. Governmental reports, conferences, pre-prints and in-house letters are some examples of grey literature according to the NATO Handbook. The recent digitalisation of most of the grey literature has, nevertheless, increased the accessibility of these sources and has consequently narrowed down the number of sources included in this sub-group.

The more recent definition provided by the RAND Corporation (2018) is already focused on a digitalised world and assumes that most if not all open sources and the variety of data/information derives from this digital environment. In consequence, RAND Corporation offers a new taxonomy of open sources, distinguishing between institutionalised sources (mass media and grey literature) and sources that are individually content-driven (social media, blogs, etc.). Digitalisation is taken for granted, and there is a big emphasis on the analytic methods and the inferred data that can be extracted from those digitalised sources. Social media is the main new addition to the more classic taxonomy here, which is understandable as previous definitions were created prior to its existence. The Internet is removed from the list, and digital sources are instead sectioned in accordance with their characteristics. Commercial online databases are not addressed in RAND's definition though, creating a doubt to the reader as to whether these are considered open sources or not. Lastly, the definition provided by Stiftung Neue Verantwortung in 2023 assumes the digital world as a fact. However, after providing a generic definition of OSINT where social media is present, the think tank openly expresses that commercially available data and, furthermore, voluntary submissions of data by the private sector can also be considered open sources for some organisations.

From the analysis of the four definitions, we can realise that the term 'open sources' lacks a universally recognised definition, and that the boundaries of the notion can sometimes be difficult to establish. In

[7] NATO defines "overt human experts and observers" as people who have direct experience on a specific situation or a specific terrain. In many places of the world, it is difficult to obtain published information and some official communications may rely on second-hand reports. In those cases, an expert with experience on the ground can be valuable to get the needed insight of the situation.

particular, the rapid evolution of information technology in the last decades has created new sources that can be challenging to assess. For example, while it is generally accepted that paid-for sources such as commercial databases are *open sources* because *anyone* who pays the fee can have access to them (Koops, 2013, p. 660), this can be challenged by the RAND Corporations definition – which does not mention it as an open source, and by several private self-taught organisations (think tanks, NGOs, specialist teams) who are exploiting OSINT and collaborating with governmental institutions with seemingly no access to those databases (Freear, 2023; Wise, 2023).[8] The reasons behind a lack of access to those commercial databases can be varied. For instance, the budget cannot be sufficient. Also, commercial entities providing the datasets can delimit their services to governmental institutions only. Finally, commercial datasets are usually a mix of openly and non-openly available data provided by individuals who accepted the trade of their data by consenting to the terms and conditions and privacy notices. Can this still be called open source?

Another controversial area is the creation of fictitious identities on social media by SISs and LEAs to access specific forums or *befriend* individuals. Different organisations and oversight bodies differ as to whether those forums/profiles requiring covert access methods can still be considered open sources. The NPCC Guidelines for instance say that "contacting [in an undercover manner] individuals using social media websites" is part of the "[o]nline covert activity" of OSINT (Wells & Gibson, 2017, p. 90). Similarly, a Canadian study that interviewed several police officers in 2011 (Frank et al., 2011, p. 12) stated that typical OSINT gathering could encompass the creation of fake accounts to befriend the individual of interest or someone in their surroundings. In contrast, other voices such as the Committee for Intelligence and Security Services in the Netherlands (CTIVD) have stated the opposite. According to this Committee, the creation of a fictitious identity on social media goes beyond the mere use of an alias and must be regarded as a covert action, outside the scope of open source operations (Koops et al., 2016). This Committee, nevertheless, does not specify the differences between a *fictitious identity* and a *mere alias*. Overall, to date, there is still no universal consensus on this topic.

[8] The Ukrainian conflict is the best example of this collaboration.

A last example where the boundaries of *open sources* are blurry involves sources that are *open* or accessible only to SISs and LEAs. These sources could include, for instance, government driver and vehicle registration databases, criminal records or financial data. Several authors and practitioners have considered these databases to be *open sources* for OSINT purposes within SISs and LEAs (Layton & Watters, 2016, p. 3). However, this conceptualisation of *open sources* is open to interpretation (Wells & Gibson, 2017, p. 88).

In practice, nevertheless, LEAs and SISs often use advanced software to combine internal datasets with open sources information to get a better understanding of a situation or to enhance the predictive capabilities of the institution. Regardless of the source's nomenclature, these practices are commonly considered part of their OSINT capabilities.

Publicly available information

"Publicly available information" is a term commonly used as a synonym to OSINF as mentioned above. For example, the US Congress and the Ministry of Defence of the UK use this term in their definitions when referring to OSINF. However, the terms *open* and *available* may not always mean exactly the same thing. Indeed, it is widely accepted among practitioners and scholars that several legal and ethical limitations restrict the *availability* of information, even when this information is *open* to everyone (Lowenthal, 1998; Reagan, 2014; Reuser, 2018; Tylutki, 2018).

Some of these limitations relate to copyright and commercial requirements of vendors and are barely controversial (Lowenthal, 1998, p. 1). Others, instead, consist of human rights (especially privacy and data protection) and ethical boundaries and are still open to debate. Arno Reuser offers a good perspective on the differences between *open* and *available* information and his view about the ethical boundaries of using OSINF. Reuser states that information that is openly accessible but not intended to be open, should not be considered "publicly available information". As an example, he cites the information dumped by WikiLeaks, stating that in the absence of a clear intention by the author for publication, the material should not be considered "openly available information", and should not be used for OSINT purposes (Reuser, 2018). This was actually the way the information leaked by WikiLeaks was

treated in the US Library of Congress during 2010-2011. The SISs in the US were prohibited from using the material for their own assessments because it was still considered classified. Yet, contradictorily, this information was open and accessible to anyone with an Internet connection and of course to any foreign intelligence services (Dover et al., 2014, p. 123).

Other authors stress the legal and ethical boundaries of the uses of OSINF from a privacy and data protection perspective (Edwards & Urquhart, 2016; Nissenbaum, 2018; Rønn & Søe, 2019). As an example, Helen Nisenbaum states that making content publicly accessible is not the same as making it available for all purposes. According to her, respecting the context in which communications happen is key to assessing privacy and data protection needs (Nissenbaum, 2009).

These are only two tiny examples of the ongoing legal and ethical discussion about the uses and availability of different OSINF. However, they are enough to reflect that *openness* and *availability* do not necessarily go hand in hand.

Overt or covert intelligence?

Overt and *covert intelligence disciplines* are terms used by SISs to classify the collection methods for the production of intelligence products. *Covert intelligence disciplines* refer to practices that need clandestine means to acquire information (Saunders, 2000, p. 22). Human intelligence (HUMINT) and signals intelligence (SIGINT) are two examples that have traditionally required covert collection methods for their production. On the other hand, *overt intelligence disciplines* embrace collection methods that require no clandestine or secret means for information acquisition. Collection methods for OSINT are generally perceived as the latter (Kent, 1949, pp. 214-215; Minas, 2010, p. 9; Saunders, 2000, pp. 12–13).

Traditionally, the decision to use overt or covert collection methods has depended on whether the information sought was secret. When the information is openly accessible, it might seem reasonable to assume that no clandestine method needs to be involved to acquire it. Applying this logic to OSINT, whose raw material (OSINF) is openly accessible to everyone, OSINT has always been considered a product derived from an overt intelligence discipline.

However, as Dover *et al.* state, the *overt* notion is a misconception in regard to OSINT collection methods (Dover et al., 2014, p. 128). While some traditional information sources (e.g., radio, newspapers, etc.) allow an *overt* collection, most of the current OSINT collection methods rarely occur in an overt way despite the accessibility of the information. Collectors "may hide their interest in a conference, mask their intentions in the academic papers read or anonymize their IP address when interrogating websites" (Dover et al., 2014, p. 128). Especially in the Internet era, minimising the digital footprint and masking the collector's presence has become usual practice. Hence, the traditional notions of *overt* and *covert* may not properly represent today's differences in collection methods. While the notion *overt* can still characterise the openness of some OSD and OSINF, even the latter can be challenged in accordance with the discussion above (section "*Open sources*: what does it mean?").

In parallel, Hatfield's view of OSINT also relates to the overt vs. covert collection methods and questions the need for this distinction. As he mentions, the overall INT taxonomy is defined "in terms of its informational source – its origin's medium of transmission or acquisition" (Hatfield, 2023, p. 3). Human intelligence (HUMINT) is sourced from humans; imagery intelligence (IMINT) from images; signals intelligence (SIGINT) from signals; measurement and signature intelligence (MASINT) from specific technical sensors such as acoustic, infrared, and spectrographic. This taxonomy tries to impose order and clarity to the intelligence community and helps to understand the technical, organisational and human resources required per INT.

OSINT, nevertheless, falls outside of this order, and it is not classified according to the transmission or acquisition needs. Instead, OSINT is demarcated by a negation, as it is considered intelligence derived from information that is not under any production or distribution limitation and requires no covert action. According to Hatfield, the creation of OSINT as a stand-alone INT had been useful for practitioners to appreciate the influx of unclassified overtly available information at the brink of the Internet. However, the distinction between overt and covert is no longer valuable in today's digital environment and, in the author's view, OSINT should therefore disappear as a separate "INT". Hatfield suggests the recategorization of overtly

available sources of information into their traditional homes (INTs) to regain conceptual and analytical benefits from it. "Intelligence acquired via an image is IMINT, regardless of its degree of availability. Using commercial capabilities to measure the presence of nuclear radiation on a piece of paper is MASINT, whether it was covertly placed or originated as a publicly available newspaper in whatever remote country. Human-derived information is HUMINT, whether it was spotted, assessed, cultivated, and reported by the CIA, the BBC or any other human source" (Hatfield, 2023, p. 16). Again, the need to have distinguished overt and covert methods is questioned here.

Stand-alone intelligence vs. foundation for multi-source intelligence

Moving towards the concept of OSINT in practice, this section analyses OSINT as a stand-alone final product versus the foundation material for multi-source intelligence.

To start, the definitions provided by the OSS Academy and Joseph Nye describe OSINT as the foundation of a multi-source (also named *all-source*) intelligence product. This means that OSINT is not considered a final intelligence product, but instead, it is seen as a product integrated into an all-source process, together with other intelligence products such as SIGINT or HUMINT. The outcome of this process is an all-source actionable product that meets the requirements of users. Many practitioners and scholars support this opinion, stating that OSINT is useful as foundation material upon which other types of intelligence rest, or as material that serves to fill the gaps of fragmented covert intelligence (De Borchgrave et al., 2006, p. 12; Norton & Weaver, 2008, p. 5; Schaurer & Störger, 2013, p. 260).

However, other definitions provided by the US Congress, NPCC and Arno Reuser suggest something different. According to them, OSINT can be a final intelligence product by itself (also called "single-source intelligence"), disseminated in a timely manner, to an appropriate audience, for the purpose of addressing a specific intelligence requirement. Current technological developments and the emergence of social media networks have eased this. For example, OSINT is prioritized and used as actionable intelligence for quick responses such as for the management of natural disasters or real-time monitoring of an event (e.g. demonstrations,

international conflicts) (Backfried et al., 2012; Freear, 2023; Hogue, 2023; LCDR & USN, 2003). Furthermore, open sources might be the only directly accessible sources for actors such as international organisations (i.e. NATO, Europol, Interpol), journalists and non-governmental organisations who, beyond SIS and LEAs, are seeking intelligence (Freear, 2023; Muhammad Idrees, 2019). OSINT may play an important role as single-source actionable intelligence in these cases.

In light of the above, we can deduce that OSINT can be a final single-source intelligence product, as well as part of a multi-source intelligence process. Whether it is used one way or the other may be decided on a case-by-case basis.

OSINT as a collaborative, integrated methodology

To conclude the study of definitions, Arno Reuser offers a distinct notion of OSINT which is interesting to analyse. In his online course on open source intelligence, he defines OSINT as a "collaborative, integrated methodology and production process" (Reuser, 2018). This definition can be interpreted in two ways: (1) OSINT as a tool for institutional collaboration, and (2) OSINT as an outcome of societal collaboration.

The first interpretation is linked to institutional collaboration. SIS and LEAs are currently confronting complex threats that go beyond regional and national borders. Collaboration between and among SIS and LEAs has therefore become essential (Akhgar et al., 2015, p. 29; Martin, 2016, p. 25). In this context, being an intelligence product created through accessible information, OSINT is often considered the safest sharing option. This option allows LEAs and especially SISs to keep their inherently classified covert intelligence secret, while sharing OSINT for collaborative efforts (NATO, 2001, p. 33). Several international organisations (e.g., NATO, Europol) already use OSINT for collaboration, and the EU has also supported several projects aimed at creating a common platform for LEAs to share, exploit and analyse OSINF together (MIRROR Project; VIRTUOSO Project). However, OSINT sharing might also face some limitations. Indeed, some OSINT products, regardless of the accessibility of their sources, "may provide details of interests or intentions and should therefore be restricted in their dissemination" (NATO, 2001, p. 34)

The second of the interpretations is even broader and could go in line with R. D. Steele's understanding of OSINT which states that OSINT is a revolutionary intelligence process that allows the creation of a self-governance structure of society where all individuals take part. "All humans have access to all information all the time", and through the use of open sources, each individual can contribute to the creation of a *human mosaic* or *World Brain*. This *World Brain* allows the construction of a bottom-up structured intelligence, where publicly available information that individuals all around the world publish thanks to the Internet, can provide a continuous understanding of the world, and human interests and capabilities (R. D. Steele, 2010, p. 45).

This understanding of OSINT offers a wider view of the process and product involving OSINT in comparison with other definitions. First, it maximises the capacities of the Internet (to a utopian degree, perhaps) – something unimaginable in a definition of OSINT provided 30 years ago. Second, it includes the participation of the whole society (and each individual) in the creation of intelligence, a characteristic that none of the other definitions mention. While it sounds utopian to a degree, we can already taste this notion of OSINT through the so-called *crowdsourcing*, where individuals voluntarily collaborate and report incidents to LEAs, and the latter ask for help from citizens through social media. The London Riots in 2011 were one of the first examples of crowdsourcing (Couts, 2011; Hobbs et al., 2014). However, the best example is probably the currently ongoing conflict in Ukraine and the expanded, even revolutionised OSINT practices seen through the year and a half of war, where civil collaboration and grassroots initiatives have transformed the way OSINT was conceived until now, giving credit to Steele and Reuser's notion of it (Hogue, 2023; Perrot & Cadenza Academic Translations, 2022; Wise, 2023).

Conclusions

This article showed the difficulties academics, regulators and practitioners have in achieving a commonly accepted definition of OSINT today, largely due to the challenges of keeping pace with the digital revolution and its subsequent advances in OSINT technologies and practices.

After clarifying a terminological confusion of several OSINT definitions in regard to *information* and *intelligence* terms, the article analysed the dynamism of several core features of OSINT such as *open sources* and the *availability* of the so-called "publicly available information". The need to quickly adapt to the changing digital environment creates nuances around these terms and generates differences in opinion regarding what OSINT should involve. For instance, deciding whether sources such as commercially available datasets and some social media activities (e.g., befriending someone on FB and creating a fictitious identity to join certain forums) are *open sources* is open to discussion. Similarly, understanding the ethical and legal boundaries of some of the data/information extracted from *open sources* such as leaked data or personal data are topics that are still under debate among scholars and practitioners.

The digital revolution has also impacted the more practical *overt* notion of OSINT. Today's collection methods leave footprints that require removing and masking the collector's presence from the digital world. Hence, the traditional differentiation of *overt* and *covert* intelligence may not properly represent today's collection methods any longer. At the same time, OSINT is considered by (mainly) traditional conceptions as the foundation of a multi-source intelligence product. However, OSINT has also proved to be valuable as a final product by itself, and this perspective is now gaining ground thanks to the revolutionised OSINT practices seen in the Ukrainian conflict. The latter is perhaps proof of OSINT's potential as envisioned by Reuser and Steele, where each individual start contributing to the creation of a *World Brain* that allows the construction of a bottom-up structured intelligence.

All these nuances in the understanding of OSINT have multi-dimensional implications at a practical, legal and oversight level. To start, they bring uncertainty to practitioners regarding internal procedures to follow and recruitment purposes. As a solution, Hatfield advocates for the elimination of OSINT as an INT and the reclassification of openly derived sources of information within traditional INTs for certainty. Second, these nuances also make it difficult for regulators to understand the scope and impact of OSINT practices. As the German think tank

Stiftung Neue Verantwortung and the Dutch oversight body CTIVD showed, a lack of concrete material scope of OSINT can result in legal uncertainties and a lack of proper oversight. Finally, the vagueness in terminology also affects the overall research in the field, since it is harder to study a concept that is not fully established. Tackling and exposing these differences through this article is needed first step towards a debate around a potentially commonly accepted definition of OSINT.

References:

1. Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Saskia Bayerl, P. (Eds.). (2015). *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*. Oxford, UK: Elsevier.

2. Backfried, G., Schmidt, C., Pfeiffer, M., Quirchmayr, G., Glanzer, M., & Rainer, K. (2012). *Open Source Intelligence in Disaster Management*. 2012 European Intelligence and Security Informatics Conference, 254-258. https://doi.org/10.1109/EISIC.2012.42

3. Central Intelligence Agency. (2010). *INTelligence: Open Source Intelligence. Historical Document*. https://web.archive.org/web/20200303002208/https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

4. Couts, A. (2011, August 9). "London Riots: Police use Flickr to help catch looters." *Digital Trends*. https://www.digitaltrends.com/social-media/london-riots-police-use-flickr-to-help-catch-looters/.

5. De Borchgrave, A., Sanderson, T., & MacGaffin, J. (2006). *Open Source Information: The Missing Dimension of Intelligence*. Centre for Strategic and International Studies (CSIS) - Transnational Threats Project.

6. Dover, R., Goodman, M. S., & Hillebrand, C. (Eds.). (2014). *Routledge Companion to Intelligence Studies*. London, UK: Routledge.

7. Edwards, L., & Urquhart, L. (2016). "Privacy in public spaces: What expectations of privacy do we have in social media intelligence?" *International Journal of Law and Information Technology*, 24, 279–310. https://doi.org/10.1093/ijlit/eaw007.

8. European Union Funded H2020 Project, Grant Agreement No 832921. (n. d.). MIRROR Project. https://h2020mirror.eu/.

9. EUROSINT Forum, European FP7-funded project. (n. d.). VIRTUOSO Project. https://www.eurosint.eu/virtuoso-project.

10. Frank, R., Cheng, C., & Pun, V. (2011). *Social Media Sites: New Fora for Criminals, Communication, and Investigation Opportunities* (021.2011). Public Safety Canada. http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf.

11. Freear, M. (2023, March 14). *OSINT in an Age of Disinformation Warfare*. RUSI.Org.

12. Hatfield, J. M. (2023). "There Is No Such Thing as Open Source Intelligence." *International Journal of Intelligence and Counterintelligence*, 1-22. https://doi.org/10.1080/08850607.2023.2172367.

13. Hobbs, C., Moran, M., & Salisbury, D. (Eds.). (2014). *Open Source Intelligence in the Twenty-First Century – New Approaches and Opportunities*. London, UK: Palgrave Macmillan.

14. Hogue, S. (2023). "Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War." *Surveillance & Society*, 21(1), 108–112. https://doi.org/10.24908/ss.v21i1.16255.

15. Kent, S. (1949). *Strategic Intelligence for American World Policy. Princeton*, New Jersey, US: Princeton University Press.

16. Koops, B. J. (2013). "Police Investigations in Internet open sources: Procedural-law issues." *Computer Law & Security Review*, 29, 654–665.

17. Koops, B. J., Roosendaal, A., Kosta, E., van Lieshout, M., Oldhoff, E., & Hildebrandt, M. (2016). TNO 2016 R10150-rapport – Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdienstein 20XX (p. 186). TNO innovation for life, Report for the Dutch Ministry of Internal Affairs.

18. Layton, R., & Watters, P. A. (Eds.). (2016). *Automating open source intelligence: Algorithms for OSINT*. Elsevier/Syngress.

19. LCDR, T. N., & USN, P. (2003). *Open Source Intelligence – Doctrine's neglected child*. Rhode Island, US: Naval War College.

20. Lowenthal, M. M. (1998). *Special Reports – Open Source Intelligence: New Myths, New Realities.* Washington D.C., US: Defence Daily Network Special Reports.

21. Martin, S. (2016). *Spying in a Transparent World: Ethics and Intelligence in the 21st Century*, 19/16 Research Series. GCSP. https://dam.gcsp.ch/files/2y10IFJfn5WfxlznHTeypxCeKNqdi9ptdONTckNIjqiSTuxCdF8PFXy

22. Minas, H. (2010). *Research Paper No. 39: Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?* Research Institute for European and American Studies (RIEAS), 59.

23. Ministry of Defence (UK). (2011). *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. Ministry of Defence Development, Concept and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

24. Muhammad Idrees, A. (2019, June 10). "Bellingcat and how Open Source Reinvented investigative journalism." *The New York Review*. https://www.nybooks.com/daily/2019/06/10/bellingcat-and-how-open-source-reinvented-investigative-journalism/.

25. National Defence Authorization Act for Fiscal Year 2006 – Intelligence Community Directive Number 301, Pub. L. No. 109–163, ICD 301.

26. National Police Chief Council. (2015). NPCC Guidance on Open Source Investigation /Research. Police Forces in England and Wales.

27. NATO. (2001). Open Source Intelligence Handbook.

28. Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* California: Stanford University Press.

29. Nissenbaum, H. (2018). *Respecting Context to Protect Privacy: Why Meaning Matters. Science and Engineering Ethics*, 24(3), 831-852. https://doi.org/10.1007/s11948-015-9674-9.

30. Norton, R. A., & Weaver, G. S. (2008). *Open Source Intelligence and Technology – A Natural Nexus for Academia and the Intelligence Community*. Auburn, Alabama, US: Auburn University.

31. Omand, D., Bartlett, J., & Miller, C. (2012). "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security*, 27(6), 801-823. https://doi.org/10.1080/02684527.2012.716965.

32. Pallaris, C. (2008). *Open Source Intelligence: A Strategic Enabler of National Security*. CSS Analyses in Security Policy, 3(32), 3.

33. Perrot, S. & Cadenza Academic Translations. (2022). *L'Open Source Intelligence dans la guerre d'Ukraine: Politique Étrangère*, Automne (3), 63-74. https://doi.org/10.3917/pe.223.0063.

34. Reagan, C. M. L. (2014). *Terms & Definitions of Interest for Counterintelligence Professionals – Glossary (Unclassified).* Department of Defense (DoD) of the US.

35. Reuser, A. (2018, May 21). *Online course on Open Source Intelligence. IntelHub.* https://www.apus.edu/academic-community/intelhub/events#reuser.

36. Rønn, K. V., & Søe, S. O. (2019). *Is social media intelligence private? Privacy in public and the nature of social media intelligence. Intelligence and National Security,* 34(3), 362–378. https://doi.org/10.1080/02684527.2019.1553701.

37. Sands, A. (2005). "Integrating Open Sources into Transactional Threat Assessments." In J. E. Sims & B. Gerber (Eds.), *Transforming U.S. Intelligence*. Georgetown, US: Georgetown University Press, p. 64.

38. Saunders, K. (2000). *Open Source Information – A True Collection Discipline* [Master Thesis]. Master of Arts (War Studies) – Royal Military College Canada.

39. Schaurer, F., & Störger, J. (2013). "The Evolution of Open Source Intelligence (OSINT)." *Journal of U.S. Intelligence Studies*, 19(3), 4.

40. Steele, R. D. (2010). *Intelligence for earth: Clarity, integrity, & sustainability*. Earth Intelligence Network.

41. Steele, R., & Lowenthal, M. (1998). *Open Source Intelligence: Private Sector capabilities to Support DoD Policy, Acquisitions, and Operations.* Defence Daily Network Special Report. https://fas.org/irp/eprint/oss980501.htm#N_1. Accessed 27 May 2020.

42. Tylutki, K. (2018). "The information of a mass destruction range – OSINT in intelligence activities." *Internal Security Review* 19/18, 384-404.

43. Wells, D., & Gibson, H. (2017). *OSINT from a UK perspective: Considerations from the law enforcement and military domains.* In Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union (pp. 84–113). Estonian Academy of Security Science.

44. Wetzling, T., & Dietrich, C. (2022). *Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?* Germany: Stiftung Neue Verantwortung.

45. Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (osint) for the defense enterprise*. Santa Monica, US: Rand Corporation.

46. Wise, J. (2023, March 4). "The DIY Intelligence Analysts Feasting on Ukraine Meet the would-be Jack Ryans of OSINT." *New York Intelligencer*. https://nymag.com/intelligencer/2022/03/the-osint-analysts-feasting-on-ukraine.html.

CYBERSECURITY

BETWEEN GLOBAL VULNERABILITIES AND REGIONAL REALITIES: CYBERSECURITY DYNAMICS IN EASTERN EUROPE

Dragoș VETRESCU[*]

Abstract:
In the vast, unbounded domain of cyberspace, the concept of regional dynamics often seems overshadowed by its inherent global nature. However, the Eastern European digital landscape presents a compelling case for recognizing and understanding the significance of regional cybersecurity nuances. This article delves into the unique cyber threats faced by Eastern Europe, influenced by intertwined state relations, particularly the pervasive cyber influence of Russia. It highlights shared vulnerabilities resulting from common technological infrastructures, interlinked economies, and mutual dependencies that make the region a collective cyber target. Furthermore, the article discusses the external shaping forces, such as the regulatory influence of the European Union and the strategic involvement of global powers like the US, in strengthening the region's cyber defences. By juxtaposing the global essence of cyberspace with the discernible regional contours in Eastern Europe, this article underscores the importance of a regional perspective in formulating nuanced, effective cybersecurity strategies.

Keywords: *Near-abroad, Cyber security, Regional Security Complex*

Introduction

Amid the vast, borderless expanse of cyberspace, where geographical markers seem almost redundant, the idea of a regional cybersecurity complex may initially sound incongruous. Cyberspace inherently erases traditional territorial demarcations, presenting a landscape where every node, regardless of its physical location, is equally accessible to threat actors. Given this level playing field, one might assume that cyber threats, devoid of the constraints of physical

[*] PhD student, SNSPA Bucharest, email: dragos.vetrescu.20@drd.snspa.ro

space, would be uniformly global, not bound or majorly influenced by regional dynamics. This presumption finds further backing in the evidence that cybercriminals, hacktivists, or even state-backed entities can orchestrate their operations from any corner of the world, targeting nations irrespective of geography or historical contexts. However, upon deeper introspection, specific regional contours emerge in the cybersecurity landscape, demanding a shift from a purely global perspective to a nuanced regional one.

The Eastern European countries considered by Russia its "near-abroad" offer a vivid illustration of this regional dynamics. Here, the entwined state-to-state relations amplify common cyber threats. The prevalent Russian influence, marked by its persistent and sophisticated cyber campaigns, underscores the unique threat landscape of the region. Such state-sponsored activities, particularly from Moscow, not only underscore the geopolitics of the region but also point to the region-specific cyber threats it faces. States in this region, while participating in a global digital environment, exhibit common vulnerabilities arising from similar technological choices, shared infrastructure, and interlinked economies. Such shared vulnerabilities make the region a collective target, with repercussions in one state potentially rippling through its neighbours.

Furthermore, the intersection of Eastern European states with entities like the European Union shapes its cybersecurity posture. The EU's regulatory norms, especially around cybersecurity, exert a significant influence, harmonizing cybersecurity measures across member states and even influencing non-member neighbouring countries. At the same time, global powers, particularly the US, play an instrumental role, fortifying the region's cyber capacities both bilaterally and under NATO's aegis. The US's dedicated efforts to build cybersecurity resilience in Eastern Europe, from capability enhancement to joint cyber exercises, magnify the role of global powers in shaping the regional cyber landscape.

In essence, while the global nature of cyberspace remains an undeniable reality, regional undercurrents, defined by geopolitics, shared vulnerabilities, and external influences, play a pivotal role in determining the cyber threat landscape of specific areas. Recognizing and understanding these regional nuances can pave the way for more

informed, collaborative, and effective cybersecurity strategies, tailored to address the unique challenges of each region. Eastern Europe, with its intricate web of state relations, external influences, and shared digital dynamics, stands as a testament to the value of conceptualizing cybersecurity through a regional lens.

This article aims to explore the regional cybersecurity dynamics in Eastern Europe, focusing on the intersection of geopolitical influences, shared technological vulnerabilities, and external interventions. Utilizing a theoretical framework grounded in the regional security complex (RSC) theory, the study employs a qualitative analysis of state-to-state cyber interactions, historical cyber incidents, and the influence of major powers, particularly the EU and the US, to understand the unique cybersecurity challenges and strategies within this specific geopolitical context.

What constitutes a Regional Security Complex (RSC)

The theory of the regional security complex is intricately linked to the framework of the English School of international relations. This connection is especially evident in the works of one of its foremost proponents, Barry Buzan. In his seminal work "Regions and Power," Buzan distinguishes between three principal theoretical perspectives on the Post-Cold War international security structure: the neorealist, globalist, and regionalist perspectives (Buzan & Wæver, 2004, p. 6). He particularly gravitates towards the regionalist perspective. While this viewpoint shares certain parallels with the prior two, it differentiates itself based on its regional focus as opposed to a state or global focus. It also varies in its understanding of the mechanisms underpinning security.

The regional perspective as envisaged by Buzan is rooted in his prior research and writings. It adopts a constructivist stance on the emergence and cessation of threats to security. As articulated by Buzan, "the formation and operation of RSCs hinge on patterns of amity and enmity among the units in the system" (Buzan & Wæver, 2004, p. 40). This implies that regional systems are not merely deterministic reflections of power distribution but are contingent upon the actions and interpretations of the involved actors.

Therefore, while the security complex theory retains a significant realist foundation, it also incorporates more liberal concepts (Wunderlich, 2016, p. 39). These include ideas such as security communities and the consequential roles of regional regimes and institutions.

The theory of the regional security complex offers a complementary lens to other international relations theories, enhancing their depth and reducing oversimplification, especially when addressing global issues. By zeroing in on regional dynamics, it provides a more nuanced perspective. The emphasis on the regional level arises from the pragmatic observation that, while there has been a pronounced focus on states as the primary objects of security (Buzan et al., 1998, p. 36), the national security of any state is intrinsically linked to that of its neighbours. As security dynamics are fundamentally relational, the security of any nation cannot be isolated from its surroundings. This idea is encapsulated in the thought that "no nation's security is self-contained" (Buzan et al., 1998, p. 43). In the realm of regional security complex theory, the crux lies in examining the relationships states and societies maintain in terms of vulnerabilities and threats.

Furthermore, as outlined by Buzan and his colleagues, as the international power dynamic becomes "more diffuse" (Buzan et al., 1998, p. 11) and major powers show increasing hesitancy to undertake political commitments in distant regions – unless their core interests are directly and intensely impacted – it's anticipated that international relations will adopt a more regional-centric tone. This shift means regions may increasingly find themselves navigating their challenges more autonomously.

The regional security complex (RSC) theory posits that viewing global security – emphasizing the international system as a whole – as a tangible reality is more an "aspiration than a reality" (Buzan & Wæver, 2004, p. 43). In comparison to the national and global dimensions, the regional level emerges as the critical juncture where these two extremes intersect and witness the most significant activity. Wunderlich underscores this notion, stating, "although all states are enmeshed in a global web of security interdependencies, insecurities are usually associated with geographic proximity" (Wunderlich, 2016, p. 39). Steward-Ingersoll and Frazier pinpoint another rationale highlighting

the primacy of regional security concerns for most states: the simple fact that "most states do not have the capacity to project force beyond their immediate neighbourhood" as "power degrades across distance" (Stewart-Ingersoll & Frazier, 2012, p. 5).

Importantly, security complexes should be perceived as "regions as seen through the lens of security" (Buzan & Wæver, 2004, pp. 43–44). They might not always align with traditional geographic boundaries. This perspective ensures adaptability in the concept of security regions, allowing them to evolve over time – a crucial consideration, for instance, when dissecting the European RSC. However, these regions are not arbitrarily delineated. Buzan emphasizes that "RSCs define themselves as substructures of the international system by the relative intensity of security interdependence among a group of units, and security indifference between that set and surrounding units" (Buzan & Wæver, 2004, p. 48).

So, how does Buzan conceptualize a regional security complex (RSC)? At its core, an RSC is defined as "a set of units whose major processes of securitisation[1], desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another" (Buzan & Wæver, 2004, p. 44). This definition unmistakably carries a constructivist undertone, acknowledging the somewhat constant nature of regions in the short run, but also recognizing the potential shifts in the units' composition over time. This sense of constancy is rooted in the understanding that processes of securitisation and desecuritisation are not conjured from thin air. More often than not, they leverage pre-existing realities, such as geographical closeness. Yet, the fluidity of RSCs is justified by the evolving relationships of friendship and hostility among units within a specific RSC over time.

The emergence of RSCs stems from the dynamic interplay between the inherent anarchy and its resulting balance-of-power implications, juxtaposed with the imperatives of geographical vicinity (Buzan & Wæver, 2004, p. 45). This unique interaction, set against a

[1] A term connected to the Copenhagen School, which designates a rhetorical process through which a problem is presented as an existential threat and thus justifies the taking of measures which would be outside normal political procedures (Buzan et al., 1998, pp. 23–26)

backdrop of geographical closeness, catalyses developments that mold the RSC. The units ensnared in this balance-of-power framework evolve to create intricate webs of alliances and rivalries. These "historical hatreds and friendships, as well as specific issues that trigger conflict or cooperation, take part in the formation of an overall constellation of fears, threats, and friendships that define an RSC" (Buzan & Wæver, 2004, p. 50).

Amidst their interactions, these units can inadvertently pave the way for external actors to influence or intervene in the region. However, such intervening actors are typically those with both the capability and stake, predominantly superpowers and global powers.

To dissect any given regional security complex (RSC), Buzan and Waever pinpoint four interconnected levels of analysis, which they term "the security constellation" (Buzan & Wæver, 2004, p. 51):

- *Internal Dynamics within States of the Region*: this level zeroes in on the threats or vulnerabilities experienced by states or groups of states within a specific region. For instance, a state's internal failure inherently ripples out, creating security concerns for its neighbors, regardless of whether it harbours aggressive intentions towards them.
- *State-to-State Relations*: this dimension captures the interactions, both collaborative and adversarial, between individual states within the RSC.
- *Engagement with Adjacent Regions*: this level recognizes that RSCs do not exist in isolation and focuses on their interactions and engagements with neighbouring regional complexes.
- *Influence of Global Powers*: this final layer acknowledges the often-significant impact and influence of global superpowers within the region, which can shape the RSC's dynamics and trajectories.

In addition to the aforementioned components, the concept of the "subcomplex" stands out. Serving as an intermediary stratum between individual states and the broader region, a subcomplex retains properties characteristic of an RSC. However, the defining feature of a subcomplex is that it is "firmly embedded in an RSC" (Buzan & Wæver, 2004, p. 51).

While traditional security apprehensions often focus on neighbouring states, in a security community, member states undergo a process of desecuritisation concerning their fellow members. However,

this does not imply a complete eradication of their security concerns simply by virtue of being part of a regional security community. Contrary to such a notion, the most evolved security communities today do not just dispense with security apprehensions. Instead, "the most mature cases of security communities today are not marked by a general forgetting of security concerns but rather by a conscious aggregation of them" (Buzan & Wæver, 2004, p. 57).

The near abroad as a potential Regional Security Complex

The "near-abroad" is a concept which has a deep symbolic meaning and implications. It is both about geography, and about symbolism, and is thus distinct from the general geographic vicinity. As a noun, "near-abroad" is a translation of the Russian *бли́жнее зарубе́жье* (romanized – *blizhneye zarubezhye*), a term whose origins and implications are far from established and certain. The original expression is a juxtaposition of the terms *бли́жнее* which has the meaning of "near" or "neighbour" and *зарубе́жье* which is a word composed through the combination of the noun *рубе́ж* which means "border" and the prefix за which translates as "beyond". It is not entirely clear as to how the term entered into use, Safire notes that "it was used firstly by Russians with a derogatory connotation, as indicating those areas at the periphery of the Soviet Union that, particularly towards the end of the Soviet Union, were seen as inflicting more costs on the budget of the Union than the benefits they provided" (*1994*).

The "near-abroad" would thus be comprised of the countries that are located in close geographical proximity to the Russian Federation. However, this definition, with its geographical undertones, would be inaccurate, as geographical proximity alone is not the criteria that unite the states comprising the "near-abroad". The term is more political than geographical, the uniting factor being their quality as states created by the dissolution of the Soviet Union. This title is used extensively in, and referring to, Russia and its interest, whereas the countries it aims to encompass do not recognize the validity of the designation. However, being a part of the Russian political identity, it determines the behaviour of this state towards the countries located in this geographical space. Thus, the main utility of the term is to distinguish between two different

types of foreign nations, the ones in the "near abroad" and all the others, located in varying proximity to Russia (proximity remains a relevant factor also regarding the other nations). In addition, not all countries in the "near-abroad" are considered the same in terms of their belonging to the "near-abroad", there are demonstratively different approaches to the Baltic countries, the Central Asians ones, and Ukraine or Belarus.

We could argue that the designation of a certain geographical space as "near abroad" is a speech act to refer to the terminology that the Copenhagen School borrowed from the philosophy of language. It does not only express information, but also performs the action of trying to shape perception both for the internal and the external public. It thus adds a trait to the Russian national identity, comprised of both Russians that inhabit its territory and those that inhabit its former territories, and it aims at stimulating a similar perception in neighbouring countries, which find themselves bound by ties that the dissolution of the USSR did not break. It is an attempt at continuation of the soviet common identity, as it was perceived by the Russians, centred on Russia, and with the other identities subservient, and not as equals. This designation has discursively justified a policy of dealing with the newly independent state not as fully-fledged sovereign nations „to be dealt with on an equal basis but as continuations, albeit under a new label, of the old union republics linked in different degrees of closeness (but never too loosely) to Mother Russia" (Rywkin, 2003).

The vicinity is part of the general impositions of geography that influences a state's behaviour in the international arena. All the states have a particular interest in their geographic adjacency, which represents most of the time the area where security interactions are significantly more frequent than outside this general area (Pop, 2016), and great powers are naturally sensitive about the interference of other powers in their vicinity. This certainly has been the case with NATO, and general Western institutions' expansion in the "near-abroad".

Because of the relative nature of the geographical factor together with the expanse of the Soviet Union, the "near-abroad" is far from homogenous. There are distinct geographical regions with different relations to the Russian Federation, and towards which this state has had varying goals, under the general objective to maintain some sort of

security buffer, and has employed several means to reach them, of which cyber-attacks are just one of the avatars facilitated by the technological development of societies.

We can thus distinguish between:

- **The Baltic States**: Estonia, Latvia, and Lithuania, have been constituents of the Russian Empire starting with the 18th century and, after a brief period of independence following the First World War, were annexed by the Soviet Union following the Ribbentrop-Molotov pact. They were some of the first to declare independence following the fall of the USSR, and have followed a constant policy associating themselves with the West, rejecting participation in the Community of Independent States (CIS). They are presently members of NATO and EU and thus firmly placed in the Western sphere of interest while having very vocal security concerns towards the Russian Federation. However, the Russian Federation still has significant leverages to pressure them, particularly in the economic sphere, where the energy infrastructure is still interconnected. Also, the number of ethnic Russians in these countries is approximately one million, and they form a significant minority particularly in Estonia (24% of the population) and Latvia (25% of the population).
- **Central Asia:** Kazakhstan, Kirgizstan, Turkmenistan, and Uzbekistan have become a part of the Russian Empire during its expansions of the 18th and 19th centuries, and have been the last to proclaim independence. They are commonly characterized by the existence of authoritarian regimes that have been established after the fall of the Soviet Union. They are members of CIS to varying degrees part of Russian-promoted international organizations. The Russian Federation has historically acted in order to keep them as part of its sphere of influence, minimize Western influence (but it encountered significantly lower pressure than in Europe), and preventing the spread of instability from Afghanistan (Dubnov, 2018). However, the area has become of interest to China, which promises significant investments as part of its Belt and Road Initiative, an evolution that could strain the Russian influence in these countries.
- **The Caucasus:** Azerbaijan, Armenia, Georgia have entered into the componence of the Russian Empire in the late 18th, early 19th

century, and have always been somewhat of a powder keg of Russia. The three states have very different approaches to Russia, varying from very close, bordering complete dependence from a security point of view in the case of Armenia, to a respectfully balanced approach towards Russia and other powers in the case of Azerbaijan, and to a hostility that has led to conflict in the case of Georgia (Mammadov & Garibov, 2018). Russia still considers the area relevant to its national security, being concerned mainly about Western infiltration in the area, and has proved that it is willing to use force to prevent this.

- **Eastern Europe:** Belarus, Moldova, and Ukraine comprise together the most complex and problematic region, as they are not only part of the particular sphere of interest that is the "near-abroad", but also of arguably more importance as being on the main historical invasion route into Russia by European powers, and thus they ensure the strategic depth that protects Moscow (slightly less so in the case of Moldova). Moldova is a country that has a large (in proportion to its population) Russian speaking minority, and, at the moment, also as a consequence of the war in Ukraine, is on an accelerated Western path. Transnistria, as a breakaway self-proclaimed republic recognized by no state, but supported by Russian, together with the presence (despite International Law and Moldovan official demands) of Russian troops in this territory significantly impairs any real move outside Russian orbit. On the other hand, political turmoil aside, the situation in the country is stable and so it does not occupy an important place in Russian security interest.

Belarus is a Russian speaking nation and has been under the rule of the Lukashenko regime since 1994. The country was placed from the beginning in the Russian sphere of influence, a fact that Belarus not only didn't dispute but has at times manifested more interest in a closer relationship with the Russian Federation than Russia was willing to offer. The two countries have formed a Union in name but not in nature, and presently there is no clear direction of this political project.

Ukraine has also pivoted between East and West, but, as a consequence of its history as a frontier region of many empires, has accumulated fault lines between various regions that were activated when the country was on the verge of placing itself to firmly on a pro-Western path. Ukraine has always had an uneasy relationship with its

Eastern neighbour with which it was connected by a myriad of dependencies, most important economically and socially/culturally. Russia considers Ukraine a strategically important area, geopolitically important, and whose full sovereignty is unacceptable. The space occupied by Ukraine is also the cradle of the Kievan Rus from whence Russia draws its roots, so its loss would be unacceptable for the Russian Federation from multiple points of view. Thus, it accepted the potential consequences for the annexation of its territory, and even for its invasion, which turned into a protracted, costly conflict for both sides.

Thus, the "near-abroad" is not a unitary regional security complex at present time, but is actually a complex region where Belarus, Ukraine and Moldova together with the Russian Federation are the main constituents. The Baltics have become part of the EU-Western RSC thus facing at the moment many of the cyber threats (mostly espionage related) which generally target NATO member states. The Caucasus and Central Asia continue to be of interest for the Russian Federation, and arguably still a part of the "near-abroad", but their importance at the moment for Russia is diminished as the war in Ukraine continues to absorb most of its resources. This dynamic is evident in the case of the recent conflict between Armenia and Azerbaijan over Nagorno-Karabakh, where Moscow's involvement was minimal in spite of the killing of Russian peace-keepers. These dynamics are also observable in cyberspace, where countries face similar, or distinct threats based on their belonging to a specific RSC.

Real space vs cyberspace - the behaviour of states in cyberspace

Cyberspace is a term that has entered common parlance, although there are real challenges to us being able to truly discern what it refers to. Indeed, even the person that is credited with the invention of the term, the science fiction author William Gibson, has described it as "evocative and essentially meaningless" (Neale, 2000). Although as the Internet has begun as a project aimed at maintaining the availability of communication for the US government in the aftermath of a nuclear attack and there has arguably always been an involvement of the US national security apparatus in shaping its workings, this communication medium has been considered as an open medium where security came secondary if it were

a consideration at all. This has recently changed and as Dunn Cavelty notes "the securitization of cyberspace is perhaps the most important force shaping global communications today" (2016).

One of the most defining and essential characteristics of cyberspace is its intangibility, which stands in stark contrast to the physicality of conventional spaces. However, the intangibility is not total. Cyberspace is man-made, and runs on man-made, physical infrastructure, which ultimately behaves the same as other physical infrastructures. Cyberspace's infrastructure, including data centres, cloud storage facilities, and undersea cables, and is far from neutral. Ownership, control, and access to this infrastructure can determine data flow, storage, and retrieval.

Cyberspace is also fundamentally interconnected as it is constituted of extensive networks and connections that facilitate the rapid flow of information across various platforms, devices, and borders. In cyberspace, interconnectedness goes beyond mere technological links; it is the intrinsic fabric that allows for extensive global communication and integration. This quality enables real-time interaction, collaboration, and data exchange between users, irrespective of geographical locations.

In the lexicon of modern cyber warfare and espionage, few terms have garnered as much attention, and at times, notoriety, as "Advanced Persistent Threats" or APTs. To understand the seismic shifts in the landscape of state-sponsored espionage in the 21st century, one must delve deep into the world of APTs, the motivations driving them, and the intricate webs of state and non-state actors that employ them.

APT is an abbreviation of the term Advanced Persistent Threat, coined to illuminate some of the main characteristics of this kind of sophisticated cyber actor:

- *Advanced* – refers to the high degree of sophistication of their tools and modus operandi, which are usually accessible to some organizations and states due to the cost and resources involved.
- *Persistent* – refers to the fact that the actors have (in most cases) a persistent interest regarding a certain target and will be able to sustain an attack until they achieve their objective, but also to the fact that most Computer Network Operations (bar some types of operations aimed at creating effects in the short term) are aimed at creating some

sort of persistent access in the victim infrastructure, whether for intelligence exfiltration or as a backdoor for future operations.

To build on previously mentioned issue, there is no commonly agreed taxonomy regarding the types of activities states conduct in cyberspace, and the characteristics of the domain make it such that there is just partial overlap with our previous experience regarding power projection in the physical space (Singer & Cole, 2020). To clarify this issue, we will adopt the model proposed by (Monte, 2015) to distinguish between types of Computer Network Operations (CNO):

- *Computer Network Exploitation* (CNE) – which encompasses all activities aimed at the exfiltration of data from networks, activities that are commonly referred to as cyber espionage.
- *Computer Network Attack* (CNA) – which refers to various activities aimed at some type of modification of the target network. It applies to the destruction, denial, degradation, or destruction of some kind of target, whether it belongs to the cyber domain or not (e.g., economic or politically relevant targets). Thus cyber-attacks can also be a form of "political signalling" (Nye, 2017).
- *Computer Network Defence* (CND) – which comprises activities aimed at the protection of the networks belonging to the defender.

The argument for a regional cybersecurity complex

When examining the intrinsic nature of cyberspace, the concept of a regional cybersecurity complex might initially appear paradoxical. One of the foundational attributes of cyberspace is its borderless environment, where geographical demarcations are rendered inconsequential. Unlike conventional territorial domains, cyberspace epitomizes a truly global expanse, transcending physical boundaries and national jurisdictions.

This universal characteristic of cyberspace engenders a unique security paradigm. In the traditional geopolitical arena, as previously mentioned, threats often manifest based on geographic proximity or historical animosities, but in cyberspace, threat actors can, with relatively equal ease, target entities across vast distances without the need for physical ingress. Such a capability fundamentally alters the threat landscape. Furthermore, the pervasive nature of cyber threats underscores the global magnitude of the challenge. Cybercriminals,

hacktivists, or state-sponsored entities can operate from virtually any location, targeting any nation irrespective of geographical, cultural, or political affinities. This omnipresence of threats means that nations cannot solely rely on regional alliances or strategies to secure their digital domains.

However, with the aforementioned caveats, there are certain regional dynamics in cybersecurity that make the case for thinking regionally about challenges and responses:

State-to-State Relations.

Just as physical regions might share common adversaries or challenges, states within a certain digital region face threats from the same cybercriminal groups or state-sponsored actors, and in the "near-abroad" by far the most significant cyber threat is posed by the Russian Federation.

The Russian Federation is widely regarded as one of the most capable actors in cyberspace, the National Cyber Power Index created by the Belfer Centre for Science and International Affairs of the Harvard Kennedy School placing it on the third position all around, and on the second position in destructive capabilities (Voo et al., 2022). This state is one of the first adopters of cyber power, enjoys multiple advantages - some historical, and some as a result of policies adopted –, and has shown great prowess in developing and utilizing cyber capabilities. The Russian Federation is credited with deploying the first "large-scale state-on-state computer network intrusion set in history", named MOONLIGHT MAZE (Rid & Buchanan, 2015)

As part of its growing assertiveness in international relations. Russia has used a wide combination of cyber instruments to:

- Obtain strategic and tactical advantages through cyber espionage.
- Undermine the cohesion of the societies of perceived adversaries by a combination of cyber intrusion and informational operations (e.g.: the use of social media by the Internet Research Agency during the US 2016 Presidential elections).
- Enhance military operations (e.g.: Georgia 2008, Ukraine).
- Ensure "information security" and, by extension, regime security (Dunn Cavelty, 2016).

The resurgence of Russian state power supported by the extra revenue from growing oil prices at the beginning of the 21st century has been accompanied by near-constant cyber operations that have targeted with predilection neighbouring countries. The extent it is willing to go to varies, but it certainly is willing to bet like it was the case with Ukraine. Also, if from a geopolitical point of view, the Baltic States are outside its sphere of influence, they are still of special interest. As part of its strategy for its neighbourhood centred on hard-power (Pop, 2016). Russia has used cyber capabilities both as a tool in itself for hard-power projection, but most times as a support for other types of capabilities.

Given the nature of the internet, Russia has always been able to project power in cyberspace globally, thus being in direct contact with strategic opponents and being able to employ a combination of the above-mentioned instruments to achieve its objectives. Public reporting by cybersecurity companies and governments have associated state-sponsored cyber-attack groups with the targeting and occasional compromise of a wide number of countries and organisations. Thus, the main APT groups that have been up until the present time attributed to Russia are:

- *APT28* (a.k.a. Fancy Bear) – publicly associated with the Military Intelligence Directorate (GRU) and involved in CNE campaigns against a variety of targets at the global level, gaining notoriety for the hacking of the US Democratic National Committee in 2016 (UK National Cyber Security Centre, 2018), but also having targets such as the Parliament of Germany in 2015 ("Germany Issues Arrest Warrant for Russian Suspect in Parliament Hack," 2020), French TV network TV5Monde in 2015 (Lichfield, 2015), the Organization for the Prohibition of Chemical Weapons (OPCW) (*Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW - News Item - Defensie.Nl*, 2018), and a series of doping-related international sports organizations (*US Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*, 2018).
- *APT29* (a.k.a. Cozy Bear) – publicly associated with either the Federal Security Service (FSB) or with the External Intelligence

Service (SVR), and reported to be involved mainly in CNE type attacks regarding targets of strategic, political interest: the DNC together with APT28 (Alperovitch, 2016), Foreign Affairs Ministries in at least three European countries (Faou et al., 2019) and as of December 2020 an impressive number of US governmental targets (Nakashima & Timberg, 2020).

- *Snake* (a.k.a. Turla or Venomous Bear) – associated with the FSB and constantly targeting diplomatic targets in Eastern Europe (Diplomats in Eastern Europe Bitten by a Turla Mosquito, 2018).
- *Gamaredon* (a.k.a. Primitive Bear) – has been associated by the Ukrainian SBU with FSB (Operation Armageddon – A Look at Russian State-Sponsored Cyber Espionage, 2015) and has been mostly targeting Ukraine related targets (Testa et al., 2020).
- *Sandworm* (a.k.a. Voodoo Bear) – named after the references to Frank Herbert's Dune series that were identified in the code of the malware. It has been associated mainly with the attacks against the Ukrainian power grid that cause an interruption of function (Lemay et al., 2018), the NotPetya Ransomware campaign in 2017, and the attack against the opening of the Winter Olympic Games in Pyeongchang in 2018 (Greenberg, 2019). It is also publicly associated with the GRU.

The most important characteristic that distinguishes the Russian behaviour in the near abroad from its general behaviour in cyber space is the willingness it manifests to use all types of operations, even CNA type attacks aimed at the disruption or destruction of some infrastructure, generally in support of some higher objective of placing political pressure or supporting the reach of some other objective. This willingness to deploy cyber capabilities that have such potentially destructive effects is a mark of both the high degree of trust regarding the effects and the possibility to contain the effects, but also of the interest for the states that comprise this region. This kind of manifest confidence also supports the assertion that the "near abroad" is not perceived as an area comprised of Westphalian sovereign states, but of political entities that have more or less liberty of action according to their

strength (here their defensive cyber capabilities) and the leverage the Russian Federation has on them. Certainly, being located in the "near-abroad" means that the probability of having to deal with a type of CNA is higher, as the only other such incidents to date have been in the Middle East and, with the exception of Stuxnet, less advanced in nature.

We also note that CNE type operations, or cyber espionage in common parlance, does not distinguish between targets in the "near-abroad" versus in the general global interest of Russia. This is to be expected from a state that has invested and relies as much on cyber capabilities for obtaining intelligence. On the other hand, it is likely that the area is placed higher in the target list and thus sees more of this type of operations. It may certainly appear so given the frequent mentioning of targets in the "near abroad" in public reporting on Russian cyber activity. However, this kind of metric is not without potential errors (maybe this is just what is reported and does not reflect reality as there are more attacks than are reported or there are more attacks directed elsewhere which are not reported) and this can be a further area of developing this research.

Internal cybersecurity dynamics within states of the region

States within a region often deploy analogous technologies, engage with a consistent pool of vendors, or might even be interconnected through shared physical infrastructures like electrical power lines or energy infrastructure. Consequently, a cyber-incident in one state – whether it is a vulnerability exploit or a direct attack – can have cascading effects on its neighbours. We have yet to see a CNA against critical infrastructure which affected neighbouring states (as this would be highly escalatory), but if we consider physical attacks, the energy interconnections between Moldova and Ukraine resulted in blackouts in both countries after a Russian missile strike ("Most Moldovan Power Supplies Restored after Russian Strikes on Ukraine," 2022). The potential for a similar regional outcome resulting from cyber-attacks is significant, as at the global level there are increasing concerns about malware pre-positioning in critical infrastructure, particularly connected to Russian state sponsored attackers (Canadian Centre for Cyber Security, 2023).

Eastern Europe is mentioned frequently as targeted by the various campaigns associated with the Russian APT ecosystem. However there is a significant difference between Moldova, which is a target of CNE and "information operations", a blend of CNOs and disinformation/ propaganda (CERT-EU, 2019), and Belarus – a sporadic target of mostly CNE, as it became on the Russia's closest allies- and Ukraine, which is the focus of multiple APT groups and a wide variety of operations.

Cybersecurity researchers have noted that Ukraine is in all accounts a cyber-testing ground, where Russia first deploys cyber capabilities and tests different potential courses of action (Greenberg, 2017). Since 2013 Ukraine has been one of, if not the main target of Russian Cyber Attacks (Cerulus 2019), so it offers many examples of both CNE and CNA, but also some operations in support of other military operations. One of the first observations we can make is that during the initial conflict with Ukraine and the occupation of the Crimean Peninsula, is that expensive cyber operation was not necessarily always the solution for obtaining objective in cyberspace. For example, during the occupation of Crimea one of the presumed objectives, obtaining control over the flow of information and blocking communications with the mainland, has been obtained simply by disrupting the Internet Exchange cables that assured the physical connection to Ukraine (Geers 2015). However here too the most relevant and concerning operations were those that aimed at producing some kind of physical effects. Three distinct operations fit this description: two directed against Ukrainian energy-producing and distribution networks (BlackEnergy in December 2015 and Industroyer in December 2016) and the most expensive and destructive ransomware to date-NotPetya, in June 2017. All three have been attributed by the US to the Sandworm group, and actually to specific officers inside the GRU ("FBI Deputy Director David Bowdich's Remarks at Press Conference Announcing Cyber-Related Indictment of Six Russian Intelligence Officers – FBI" 2020).

First in 2015 and then in 2016, in both cases during wintertime, the energy infrastructure in Ukraine has been targeted by malware that has been associated with Sandworm. The 2015 attack started on December 23rd and consisted basically of disconnecting energy substations belonging to three Ukrainian energy distribution companies, which caused a blackout for nearly 225.000 customers for more than

6hours (Greenberg 2019). In addition, given the deletion of some software components of SCADA systems, in some parts of the Ukrainian power sector, the attack meant the loss of automation for more than a year ("Crashoverride Analysis of the Threat to Electric Grid Operations" 2017). The 2016 attack also took place in December, on the 17th, and was an improvement in terms of the malware used and the objectives. Firstly, it was specifically designed to target transmission level substations in Ukraine and became the "second-ever specimen of code that directly attacked the physical world" (Greenberg 2019) after Stuxnet. As to its objectives, initial reporting ("Crashoverride Analysis of the Threat to Electric Grid Operations" 2017) suggested that its limited nature (targeting a single substation) and some characteristics of the internal code were proof that the attack was meant as a test, a "proof of concept" rather than a real cyber-attack. However, subsequent analysis (Greenberg 2019) suggests that the malware was meant to cause a second, permanent effect when the engineers tried to remedy the initial disruption. This second component appears to have failed.

The 2017 NotPetya ransomware campaign spread from a small company that offered and accounting software (M.E. Doc) in Ukraine to gain global visibility and impact. It affected systems belonging to the Ukrainian government (Health Ministry, various hospitals, the Post Office), the Chernobyl clean-up facility, the Danish Shipping company Maersk, the pharmaceutical company Merck, but also the state-owned company Rosneft, the steelmaker Evraz, the medical technology firm Invitro and Sberbank (Greenberg 2019). The attack caused 10 billion dollars in damages, and, unlike regular ransomware, it could not revert the damage (unencrypt the files). This fact, together with the fact that there was no way in which the attacker could communicate with the victims (the email address indicated was blocked by the email provider for breach of terms of service) made specialist assume that the attack was meant just to cause damage or destroy information (Goodin 2017). It likely was even more successful than the attackers assumed.

The war in Ukraine brought in its wake a wide array of cyber-attacks, most of them for cyber espionage, but also occasionally destructive in intent. The Ukrainian State Service of Special Communications and Information Protection currently tracks at least 23 groups which are considered to be Russia-led (State Service of Special Communication

and information Protection of Ukraine, 2023a, p. 12). In the context of the invasion, and to support the warfighting, destructive attacks have targeted a very wide array of industries and technologies such as the KA-SAT satellite network (Viasat, 2022), media, energy, logistic and telecom providers in Ukraine (State Service of Special Communication and information Protection of Ukraine, 2023b).

In the Baltic States, the main focus appears to be CNE type operations, aimed at exfiltrating intelligence, with CNA operations being rare but always a possibility. However, the best-known cyber-attack that took place in this region was the CNA type operation that targeted Estonia in 2007, and that made many governments wary of the disruptive and destructive potential of cyber operations. Thus, following tensions between the Estonian and Russian governments regarding the relocation in Tallinn of a statue of the Red Army soldier, the Estonian governmental, banking, and mass media infrastructure has been targeted by a *distributed denial-of-service* (DDoS)[2] type attack that paralyzed the country for the better part of two weeks. Some of the compromised websites also have been "defaced"[3], "replacing the content of websites with swastikas and pictures of the country's prime minister with a Hitler moustache, all in a coordinated effort to paint Estonians as anti-Russian fascists" (Greenberg, 2019). The attack has been attributed to Russian concern due to its interest in the matter, geopolitical reasons of state and the need for some kind of coordination, particularly to sustain the attacks, but as this kind of attacks that have a distributed infrastructure (multiple servers some belonging to civilians), the attribution is a weak one. It is to be noted that Vladimir Putin did make a veiled reference to the incident in his Victory Day speech, mentioning "those who desecrate monuments to the heroes of the war are insulting their own

[2] A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. See more on What Is a Distributed Denial-of-Service (DDoS) Attack?

[3] Web defacement is an attack in which malicious parties penetrate a website and replace content on the site with their own messages. The messages can convey a political or religious message, profanity or other inappropriate content that would embarrass website owners, or a notice that the website has been hacked by a specific hacker group. See more Imperva.

people (and) sowing discord and new distrust between states and people" (Faulconbridge, 2007).

The focus on CNE type operations is similar if we look at Central Asia, a report by Kaspersky ("A Slice of 2017 Sofacy Activity," 2018) indicating interest for a variety of targets (e.g.: science and engineering centres, Industrial and hydro chemical engineering and standards/ certification, ministries of foreign affairs, embassies and consulates, national security and intelligence agencies, press services, NGO – family and social service, ministry of energy and industry) located in all the nations component to the region. We have yet to have reported any CNA type operation in the area.

The countries of the Caucasus have mostly been targets of CNE operations that appear to be constant ("A Slice of 2017 Sofacy Activity," 2018) particularly aimed at discerning relations with NATO ("APT28 Delivers Zebrocy Malware Campaign Using NATO Theme as Lure," 2020). However, there is a distinction to be made between Armenia and Azerbaijan, who correspond firmly with this assertion, and Georgia, who has placed itself on antagonistic positions towards Moscow and has been involved in an open conflict with Russia.

The Russo-Georgian war of 2008 has been the first example of Russian use of CNOs in support of military operations. The modus operandi bears resemblance to what happened in Estonia in the previous year: a massive DDoS attack that accompanied the advance into Georgia by the Russian Army and that put out of work the websites of several central Georgian institutions (Ministry of Foreign Affairs, Presidency), the embassies of US and UK, but also those of the media and local institutions in conjunction with physical attacks against targets from different parts of the country (Greenberg, 2019). Georgia, due to its pro-Western orientation and weak cyber capability, is a recurring target of CNOs perpetrated by Russian APT's. In October 2020 the US authorities have indicted six GRU officers that are connected with the Sandworm group which they accused, among others, of "destructive, disruptive, or otherwise destabilizing computer intrusions and attacks (…) on Georgian Companies and Government Entities: a 2018 spear phishing campaign targeting a major media company, 2019 efforts to compromise the network of Parliament, and a wide-ranging website defacement campaign in 2019" (US Department of Justice, 2020).

Engagement with adjacent regions and global powers

The most important interaction in the region is that with the European Union, a normative superpower, and arguably a complex and multifaceted regional security complex on its own. The EU constitutes an institutionally centred RSC, up to the moment the security concerns of member states being dominated by their belonging to the EU. On the other hand, inside the EU RSC we can of late identify multiple sub complexes with individual, not always overlapping security concerns. Thus, the eastern periphery sees an existential threat in the resurge of Russia and the hard power instruments this state employs in its neighbourhood, a threat that is geographically distant and thus less relevant for the West or South of Europe. The South is confronted with migration and terrorism, having various failed states in its vicinity, a threat that indirectly affects the rest of Europe. The centre is in turn more preoccupied by political and economic evolutions inside the EU, trying to balance, and still maintain its control over the periphery and EU affairs, and at the same time dealing with migrant waves that aim for the economically prosperous areas.

Thus, European security continues to be marked by its perennial concern for societal evolutions but also has to balance a common response to threats that are not always felt with the same intensity. For the moment the RSC is stable, as the consequences of the changing the *status quo* are unpredictable, but arguably detrimental to European security. As more and more voices ask for internal changes, and reforms are needed in order to deal with security issues, it is expected that there will be an internal transformation, but the complexity of the RSC makes it exceedingly difficult to offer predictions on what those changes will look like.

From a cybersecurity point of view, the most important effects of the EU are in terms of regulatory influence, as EU member states and candidates adopt cybersecurity regulations like the NIS2 – Directive (EU) 2022/2555 –, aimed at boosting the overall level of cybersecurity in the EU (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) | Shaping Europe's Digital Future*, 2023). Of course, the regulations are applicable for the whole of the European Union, but they have the effect of enmeshing the EU members on the

Eastern Flank together with candidates outside the EU in a shared framework of cybersecurity policies, regulations, and norms.

The US involvement in Eastern Europe, both bilaterally and through NATO, has been characterized by a robust commitment to fortify the region's cybersecurity infrastructure and capabilities. Recognizing the evolving cyber threats that Eastern European nations face, particularly from state-sponsored actors and sophisticated cybercriminal groups, the US has embarked on a series of bilateral engagements, offering technical expertise, capacity-building programs, and information-sharing mechanisms to bolster regional cyber resilience. Concurrently, within the NATO framework, the U.S. has been instrumental in advancing the Alliance's cyber defence strategy. The establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, is a testament to this commitment, with the US playing a pivotal role in its operational success and strategic direction. Moreover, joint cyber exercises, like the annual "Locked Shields," not only underscore the collective resolve to counter cyber threats but also enhance interoperability and foster a unified cyber defence approach across the alliance. By intertwining its national strategic interests with the broader goals of NATO, the US underscores its dedication to a secure and resilient cyberspace for Eastern Europe, reinforcing the region's digital frontiers against potential adversaries.

Conclusion

The "near-abroad" is a symbolic, political rather than geographical space, a discursive construct aimed at shaping the Russian national identity and projecting influence in the ex-soviet states. The states that it refers to have as a major distinguishing characteristic their belonging to both a sphere of influence and a vital protection space, part of the strategic depth that ensures Moscow's protection. This kind of great power considerations trump the abstract principles of Westphalian sovereignty and justify interventions that could be considered a form of coercion to maintain the status quo in the region and prevent encirclement by the West.

The events in the physical space are anticipated and sometimes complemented/supported by an event in cyberspace, where Russia is one of the most capable and active players. All the neighbouring states

are a target of cyber espionage conducted by APT groups associated with Russian institutions. However, the fact that sets them apart is the probability of confronting some kind of cyber-attack aimed at disruption or destruction should their decisions be not to Moscow's liking. In this case, civilian infrastructure is both a valid and likely target. If we are to analyse the last twenty years, CNE is far more common than CNA, but there have been major incidents of attacks aimed at the disruption or destruction of infrastructure in Russia's near abroad which show that Russia is both a capable actor but more importantly one willing to employ these capabilities even when the effects are hard to anticipate (as in the case of NotPetya ransomware).

By conceptualizing cybersecurity at a regional level, policymakers can better anticipate shared threats, pool resources and expertise, and create more effective regional defense mechanisms against cyber adversaries. Moreover, understanding the interconnected nature of digital threats within a region can foster collaboration and trust among states, essential components in creating a robust collective cyber defence.

References:

1. *A Slice of 2017 Sofacy Activity*. (2018, February 20). https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

2. Alperovitch, D. (2016, June 14). *Bears in the Midst: Intrusion into the Democratic National Committee*. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

3. *APT28 Delivers Zebrocy Malware Campaign Using NATO Theme as Lure*. (2020, September 22). https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/

4. Buzan, B., & Wæver, O. (2004). *Regions and Powers: The Structure of International Security*. Cambridge University Press.

5. Buzan, B., Wæver, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

6. Canadian Centre for Cyber Security. (2023, May 12). *The cyber threat to Canada's oil and gas sector*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

7. CERT-EU. (2019). *Threat Landscape Report* (p. 4). CERT-EU. https://www.eui.eu/Documents/ServicesAdmin/ComputingService/Security/TLR2019Q1-Executive-v1.0.pdf

8. *Diplomats in Eastern Europe bitten by a Turla mosquito*. (2018). ESET. https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

9. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future*. (2023, September 27). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

10. Dubnov, A. (2018). Reflecting on a Quarter Century of Russia's Relations with Central Asia. *Carnegie Endowment for International Peace*, 13.

11. Dunn Cavelty, M. (2016). *Routledge Handbook of Security Studies* (2nd ed.). Routledge. https://doi.org/10.4324/9781315753393

12. Faou, M., Tartare, M., & Dupuy, T. (2019). *OPERATION GHOST – The Dukes aren't back – They never left* (ESET Research White Papers). ESET. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

13. Faulconbridge, G. (2007, May 9). Putin jabs at Estonia at WW2 parade. *Reuters*. https://www.reuters.com/article/us-russia-putin-estonia-idUSL0957951620070509

14. Germany issues arrest warrant for Russian suspect in parliament hack: Newspaper. (2020, May 5). *Reuters*. https://www.reuters.com/article/us-russia-germany-warrant-idUSKBN22H0TB

15. Greenberg, A. (2017, June 20). How an Entire Nation Became Russia's Test Lab for Cyberwar. *Wired*. https://www.wired.com/story/russian-hackers-attack-ukraine/

16. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Knopf Doubleday Publishing Group.

17. Imperva. (n.d.). What is a Website Defacement Attack | Examples & Prevention | Imperva. *Imperva Learning Centre*. Retrieved May 19, 2024, from https://www.imperva.com/learn/application-security/website-defacement-attack/

18. Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

19. Lichfield, J. (2015, June 10). *TV5Monde hack: "Jihadist" cyber-attack on French TV station could have.* The Independent. https://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-french-tv-station-could-have-russian-link-10311213.html

20. Mammadov, F., & Garibov, A. (2018). South Caucasus as a Regional Security Complex: Divergence of Identity and Interdependence of Security. In *Cooperation in Eurasia: Linking identity, security, and development*.

21. Monte, M. (2015). *Network attacks & exploitation: A framework*. John Wiley & Sons, Inc.

22. *Most Moldovan power supplies restored after Russian strikes on Ukraine*. (2022, November 23). Reuters. https://www.reuters.com/world/europe/half-moldova-without-power-after-russian-strikes-ukraine-deputy-pm-2022-11-23/

23. Nakashima, E., & Timberg, C. (2020, December 14). Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce. *Washington Post*. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

24. Neale, M. (2000, October 4). *No Maps for These Territories* [Documentary]. Mark Neale Productions.

25. *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW - News item—Defensie.nl*. (2018, October 4). [Nieuwsbericht]. Ministerie van Defensie. https://doi.org/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

26. Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44-71. https://doi.org/10.1162/ISEC_a_00266

27. *Operation Armageddon – A Look at Russian State-Sponsored Cyber Espionage* (p. 51). (2015). Lookingglass Cyber Threat Intelligence Group. https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf

28. Pop, A. (2016). From cooperation to confrontation: The impact of bilateral perceptions and interactions on the EU-Russia relations in the context of shared neighbourhood. *Eastern Journal of European Studies*, *7*(2), 24.

29. Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4-37. https://doi.org/10.1080/01402390.2014.977382

30. Rywkin, M. (2003). Russia and the Near Abroad Under Putin. *American Foreign Policy Interests*, *25*(1), 3–12. https://doi.org/10.1080/10803920301110

31. Safire, W. (1994, May 22). On Language. The Near Abroad – The New York Times. *The New York Times Magazine*, 16.

32. Singer, P., & Cole, A. (2020). *A Warning from Tomorrow*. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

33. State Service of Special Communication and information Protection of Ukraine. (2023a). *Russia's Cyber Tactics H1'2023* (p. 21). State Service of Special Communication and information Protection of Ukraine. https://cip.gov.ua/en/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit

34. State Service of Special Communication and information Protection of Ukraine. (2023b). *Russia's Cyber Tactics: Lessons Learned 2022* (p. 33). State Service of Special Communication and information Protection of Ukraine. https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine

35. Stewart-Ingersoll, R., & Frazier, D. (2012). *Regional Powers and Security Orders*. Routledge. https://doi.org/10.4324/9780203804995

36. Testa, D., Martire, L., & Pirozzi, A. (2020, February 17). Cyberwarfare: A deep dive into the latest Gamaredon Espionage Campaign. *Yoroi*. https://yoroi.company/research/cyberwarfare-a-deep-dive-into-the-latest-gamaredon-espionage-campaign/

37. UK National Cyber Security Centre. (2018, October 3). *Reckless campaign of cyber-attacks by Russian military intelligence service exposed*. Www.Ncsc.Gov.Uk. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

38. *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*. (2018, October 4). https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

39. US Department of Justice. (2020, October 19). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. Www.Justice.Gov. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

40. Viasat. (2022, March 30). *KA-SAT Network cyber-attack overview*. Viasat.Com. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

41. Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index 2022. *Cyber Power*.

42. *What is a distributed denial-of-service (DDoS) attack?* (n.d.). Cloudflare. Retrieved May 19, 2024, from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

43. Wunderlich, J.-U. (2016). *Regionalism, Globalisation and International Order: Europe and Southeast Asia*. Routledge. https://doi.org/10.4324/9781315604459

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY

THE HAWALA SYSTEM IN THE WESTERN BALKANS: CHALLENGES AND STRATEGIES FOR COUNTERTERRORISM AND COUNTERINTELLIGENCE

Anastasios-Nikolaos KANELLOPOULOS*

Abstract:

The Hawala system, an informal and traditional money transfer mechanism, has been a subject of concern for counterterrorism and counterintelligence agencies worldwide due to its potential exploitation for illicit financial activities, including terrorism financing. This paper provides a comprehensive examination of the Hawala system's presence in the Western Balkans, a region historically characterized by geopolitical complexity and a complex security landscape.

Drawing on empirical data and regulatory analysis, this study explores the challenges posed by the Hawala system in the context of counterterrorism and counterintelligence efforts in the Western Balkans. It examines the system's vulnerabilities, its exploitation for terrorism financing and the difficulties faced by intelligence agencies in monitoring and disrupting Hawala networks. Moreover, the paper assesses the regulatory frameworks implemented by countries in the region and offers practical policy recommendations to enhance counterterrorism and counterintelligence strategies, fostering greater security and stability in the Western Balkans.

Keywords: *Hawala, Western Balkans, Counterterrorism, Counterintelligence, Anti-Money Laundering*

Introduction

The Western Balkans, a region nestled at the Southeastern Europe, has played a pivotal role in the complex interplay of political, cultural and security dynamics (Blockmans, 2006). Its strategic location, historical legacies and ethnic diversity have rendered the Western

* PhD Candidate in Business Intelligence, Athens University of Economics and Business, Greece and Frontex CIRAM Analyst Certified, email: ankanell@aueb.gr.

Balkans a region of geopolitical significance and at times, volatility. Amidst this intricate tapestry of challenges and opportunities, one phenomenon has garnered increasing attention from scholars and security experts alike: the Hawala system. The Hawala system, an informal and ancient money transfer mechanism, has become a subject of heightened concern in the context of counterterrorism and counterintelligence efforts in the Western Balkans (Hancock, 2008).

The Hawala system's presence in the Western Balkans is far from a mere financial curiosity; it constitutes a complex and multifaceted challenge (Müller, 2012). This paper embarks on a comprehensive exploration of the Hawala system within the Western Balkans, aiming to shed light on the challenges it poses and the strategies required for effective counterterrorism and counterintelligence in this respect. The research methodology involves an extensive literature review of academic articles and public books, coupled with analysis by experts. By synthesizing information from various scholarly and professional sources, this study aims to provide a comprehensive understanding of the Hawala system within the Western Balkans. The research objective is to provide a detailed overview of the general situation regarding the Hawala system in the Western Balkans. Through meticulous analysis and synthesis of existing literature and expert insights, this study seeks to shed light on the multifaceted challenges posed by the Hawala system in the region, as well as to identify potential strategies for effective counterterrorism and counterintelligence efforts.

Background and Significance

The Hawala system's historical origins can be traced back to the Arab world and the Indian subcontinent, where it evolved as a means of facilitating remittances and trade (Jamwal, 2002). This informal financial network operates on trust, relying on a web of brokers or Hawaladars who facilitate cross-border transactions, often without the need for formal financial institutions (Müller, 2012). This system's decentralized and trust-based nature has made it an attractive vehicle for the transfer of funds, both legitimate and illicit, across the Western Balkans and beyond (Lascaux, 2014).

The Western Balkans, comprised of Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro, North Macedonia and Serbia, has long grappled with a complex blend of historical, ethnic and political tensions (Abbas, 2007). These intricacies, coupled with the region's proximity to conflict zones and its historical role as a crossroads between East and West, have rendered it vulnerable to various security challenges, including terrorism and organized crime (Gibas-Krzak, 2013).

Understanding the Hawala system's presence and operation within the Western Balkans is of paramount significance. This region has witnessed a proliferation of illicit financial activities, including money laundering, terrorism financing and the movement of funds for criminal enterprises (Lodge, 2020). The Hawala system, operating outside conventional banking channels and regulatory oversight, offers a veil of anonymity that makes it a preferred choice for those seeking to transfer funds covertly (Jamwal, 2002).

Furthermore, the Hawala system's vulnerabilities have been exploited by terrorist organizations operating in or with links to the Western Balkans. The financing of terrorism through Hawala networks presents a significant security risk that requires immediate attention. Numerous high-profile cases have underscored the need to unravel the intricacies of these systems, monitor their activities and develop effective strategies to counter their use for nefarious purposes.

This paper delves into the historical evolution, operational mechanics and vulnerabilities of the Hawala system in the Western Balkans, offering a nuanced understanding of its role in facilitating both legitimate and illicit financial transactions (Abbas, 2007). Through empirical data and regulatory analysis, utilizing meticulous analysis and synthesis of existing literature and expert insights, it examines the challenges faced by intelligence agencies in monitoring and disrupting Hawala networks. Moreover, it evaluates the regulatory frameworks implemented by Western Balkan countries and suggests practical policy recommendations to bolster counterterrorism and counterintelligence efforts in the region (Passas, 2017).

By addressing these critical issues, this paper aims to contribute to the broader discourse on security and stability in the Western Balkans and provide insights that can inform more effective strategies for countering terrorism financing and illicit financial activities (Gibas-

Krzak, 2013). It is within this context of historical complexity, geopolitical significance and evolving security threats that the Hawala system in the Western Balkans emerges as a subject of utmost relevance and urgency.

Understanding the Hawala System

The Hawala system, an ancient and clandestine money transfer mechanism, has a rich historical evolution that spans centuries and continents, rooted in principles of trust, discretion and personal relationships (Han et al., 2022). This informal financial network originated in the medieval Islamic world, primarily in regions such as the Indian subcontinent and the Arabian Peninsula, where it served as a pragmatic solution for facilitating cross-border trade and remittances. Its name, "Hawala," is derived from the Arabic term "Hawala" signifying "transfer" or "change" underscoring its central function of moving funds from one location to another, often across great distances (Passas, 2017).

Historical Evolution: The Hawala system's historical evolution is characterized by its resilience and adaptability, reflecting its capacity to navigate changing political, economic and technological landscapes. While pinpointing its exact inception remains challenging, historians suggest that the Hawala system traces its roots to the early Islamic expansion during the eighth century (Lascaux, 2014). During this period, as Muslim merchants and traders engaged in long-distance commerce, the Hawala system emerged as a means to expedite the secure movement of funds. Trusted intermediaries, known as Hawaladars, facilitated these transactions, laying the foundation for the system's principles of trust and honour (Han et al., 2022).

The Hawala system played a pivotal role during the Islamic Golden Age, a period marked by flourishing trade, cultural exchange and economic activity (Jamwal, 2002). As Islamic civilization thrived, so did the Hawala system, adapting to meet the evolving financial needs of merchants, traders and travellers (Passas, 2017). It became an integral tool for facilitating transactions across expansive trade networks, including the renowned Silk Road, connecting regions as distant as North Africa, South Asia and the Middle East (Jamwal, 2002). During this time, the Hawala system showcased its inherent flexibility and ability

to operate effectively across diverse currencies, languages and cultures (Lascaux, 2014).

With the spread of Islam and the ascendancy of Muslim empires, the Hawala system's influence expanded, gaining prominence in regions under Ottoman, Safavid and Mughal rule (Çınar, 2022). The Ottoman Empire, in particular, relied on the Hawala system to facilitate the efficient movement of funds across its vast territorial holdings and commercial interests. The system's cross-cultural adaptability enabled it to thrive in this diverse geopolitical landscape (Çınar, 2022).

In the modern era, the Hawala system adapted once again, shifting its focus from traditional trade to remittances (Jamwal, 2002). It became a lifeline for migrant workers and diaspora communities, providing them with a means to remit money to their families in their countries of origin. This transition reflects the Hawala system's ability to respond to evolving financial needs while maintaining its core principles of trust, efficiency and the swift transfer of funds.

Yet, in the 20th and 21st centuries, the Hawala system faced new challenges and opportunities. As governments and international organizations began scrutinizing its role in facilitating illicit financial activities, including terrorism financing and money laundering, regulatory efforts emerged to formalize and monitor aspects of the system (Han et al., 2022). This led to a complex interplay between traditional practices and modern financial regulations, with the Hawala system both adapting to new realities and grappling with increased scrutiny (Lodge, 2020).

Operational Mechanics: The operational mechanics of the Hawala system are as intricate as they are discreet, grounded in a network of trust-based relationships. Its key operational steps are as follows:

1. Initiation of a Transaction: A sender (client) approaches a local Hawaladar to initiate a transaction, specifying the amount of money to be transferred and providing details about the recipient, including their name and location (Jamwal, 2002; Müller, 2012). These transactions are often conducted verbally, without the need for written documentation (Lascaux, 2014; Çınar, 2022).
2. Authentication and Verification: Trust is fundamental to the Hawala system. The sender and Hawaladar typically share an established relationship, often built over years of doing business together or through referrals from trusted sources (Hancock,

2008). This personal connection serves as a form of authentication, with the Hawaladar verifying the sender's identity and the legitimacy of the transaction (Passas, 2017).

3. Recording the Transaction: While Hawala transactions are frequently verbal agreements, Hawaladars often maintain meticulous records of their transactions, often in ledgers or through modern record-keeping methods (Jamwal, 2002). These records serve both as a reference for the Hawaladar and as a means of tracking the flow of funds (Hancock, 2008).
4. Payment to the Recipient: Upon verification of the transaction, the Hawaladar in the sender's location contacts a corresponding Hawaladar in the recipient's location (Müller, 2012). The sender's Hawaladar provides the recipient's details and the agreed-upon amount. The recipient's Hawaladar then contacts the recipient, who is often provided with a unique code or password to confirm their identity (Hancock, 2008). Once authenticated, the recipient is paid the transferred amount, usually in the local currency (Lascaux, 2014).
5. Settlement among Hawaladars: After the recipient receives the funds, the two Hawaladars involved in the transaction settle their accounts (Müller, 2012). Settlement can occur through various means, including offsetting transactions, cash payments or even non-financial arrangements (Çınar, 2022). This step is crucial for maintaining trust and equilibrium within the Hawala network (Passas, 2017).
6. Commission Fees: Hawaladars typically charge commission fees for their services, varying based on factors such as the amount transferred, the distance between the sender and recipient and the perceived risk of the transaction. These fees are typically deducted from the transferred amount (Jamwal, 2002).
7. Anonymity and Secrecy: An essential characteristic of the Hawala system is its emphasis on confidentiality and discretion (Hancock, 2008). Transactions are conducted privately and participants often prefer to remain anonymous to avoid attracting undue attention (Çınar, 2022). While this secrecy has legitimate applications, it has also raised concerns among authorities about potential misuse for illicit activities (Passas, 2017).

Counterterrorism and Counterintelligence in the Western Balkans

Counterterrorism and counterintelligence efforts in the Western Balkans constitute a multifaceted and dynamic challenge, caused by the region's historical complexities, ethnic diversity and geopolitical significance (Đorđević et al., 2018; Heineman and Nomikos, 2022). The Western Balkans, comprised of countries such as Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro, North Macedonia and Serbia, has faced a range of security threats, including terrorism, organized crime and extremist ideologies (Abbas, 2007; Herbert, 2022). In response to these challenges, both domestic and international actors have mobilized to confront and mitigate these threats (Kudlenko, 2019).

Subsequently, Western Balkans historically marked by a mosaic of cultures, religions and political structures, has often been a crucible of conflicts and tensions (Blockmans, 2006). The disintegration of Yugoslavia in the 1990s led to a series of brutal ethnic conflicts that left scars on the region's social fabric (Gibas-Krzak, 2013). These conflicts, coupled with the collapse of authoritarian regimes in some Balkan states, created a fertile ground for the emergence of extremist ideologies and armed groups (Arsovska, 2019).

The region's vulnerability to terrorism threats is exacerbated by several factors, including its proximity to conflict zones in the Middle East, a history of inter-ethnic tensions and economic challenges (Richards, 2018). Notably, the Western Balkans has been identified as a source of foreign fighters joining terrorist organizations in Syria and Iraq, leading to concerns about radicalization and the potential return of battle-hardened extremists (Gibas-Krzak, 2013). Moreover, the region has seen the emergence of home-grown extremist movements and networks, some with transnational ties, contributing to a complex security landscape (Blockmans, 2006; Đorđević et al., 2018).

To address these threats, Western Balkan countries have implemented a range of counterterrorism strategies (Abbas, 2007). These strategies encompass legal reforms, intelligence sharing, law enforcement cooperation and countering violent extremism (CVE) programs. Regional organizations, such as the Southeast European Law Enforcement Centre (SELEC) and the Regional Cooperation Council

(RCC), have played vital roles in facilitating information exchange and collaboration among Western Balkan states (Blockmans, 2006; Proksik, 2017). Furthermore, some countries have adopted comprehensive CVE approaches, focusing on preventing radicalization and promoting deradicalization and reintegration (Bures, 2010).

However, numerous challenges and obstacles persist in the region's counterterrorism efforts. These include limited resources, capacity gaps in law enforcement and intelligence agencies, porous borders and issues related to the rule of law and corruption. The Western Balkans' complex ethnic and political landscape can also complicate cooperation and information sharing among states (Kudlenko, 2019).

Given the transnational nature of terrorism threats, international partners, including the European Union (EU), the United Nations and the United States, have provided substantial support to Western Balkan countries in their counterterrorism endeavours (Kudlenko, 2019). The EU, in particular, has played a pivotal role in promoting regional cooperation, offering financial assistance, and providing technical expertise to strengthen the region's counterterrorism capabilities (Herbert, 2022).

In addition to counterterrorism, counterintelligence efforts in the Western Balkans are crucial for safeguarding national and regional security (Foertsch, 1999). These efforts aim to detect, deter and mitigate espionage activities, unauthorized disclosure of classified information and the infiltration of foreign intelligence agencies. Given the region's historical and contemporary political complexities, counterintelligence is essential for preserving state sovereignty and protecting critical infrastructure (Heineman and Nomikos, 2022).

Counterintelligence in the Western Balkans faces its own set of challenges, including a legacy of mistrust and historical animosities among neighbouring countries, as well as the presence of foreign intelligence agencies seeking to exert influence and gather sensitive information (Heineman and Nomikos, 2022). The porous borders and fluid political dynamics in some Western Balkan states create opportunities for intelligence activities that threaten national security (Hughes, 1982; Foertsch, 1999).

Effective counterintelligence relies on coordination and information sharing among intelligence agencies at the national and regional levels (Foertsch, 1999). Building trust and cooperation among intelligence services is essential for detecting and countering espionage threats (Hughes, 1982). International partnerships, including those with NATO and EU intelligence bodies, contribute to strengthening counterintelligence capabilities in the Western Balkans (Heineman and Nomikos, 2022).

Hawala system in Albania, Kosovo, North Macedonia and Montenegro

The Hawala system has deep-rooted historical and cultural significance in the Balkan region, including Albania, Kosovo, North Macedonia and Montenegro. These countries share historical, cultural and linguistic ties, which have facilitated the spread and continuity of the Hawala system across borders (Liargovas and Repousis, 2011; Arsovska, 2019). In this region, Hawala operates as an essential financial lifeline for communities, serving as an efficient means of transferring funds and conducting transactions, especially in areas with limited access to formal banking services (Han et al., 2022).

In Albania, Kosovo, North Macedonia and Montenegro, the Hawala system has played a significant role in mitigating economic challenges and facilitating cross-border trade and remittances (Arsovska, 2019). This informal network relies heavily on trust and personal relationships within close-knit communities (Hancock, 2008).

One key aspect of the Hawala system in this region is its role in diaspora communities. Many Albanian and Kosovar communities have established themselves abroad, particularly in Western Europe and the United States. The Hawala system serves as a conduit for remittances sent by Albanian and Kosovar diaspora members to support their families back home. This flow of remittances contributes significantly to the local economies of these countries and provides a lifeline for households (Liargovas and Repousis, 2011).

Despite its economic importance and cultural significance, the Hawala system in these Balkan countries also faces challenges. Its informality and lack of regulation raise concerns about the potential misuse for illicit financial activities, such as money laundering and

terrorism financing (Lodge, 2020). To address these challenges, governments in the region have taken steps to implement anti-money laundering and counterterrorism financing (AML/CTF) regulations. However, harmonizing these regulations across borders and fostering international cooperation remain complex tasks.

Efforts to regulate the Hawala system must strike a balance between preserving its legitimate role in facilitating financial transactions and preventing its misuse for illegal activities. Authorities in Albania, Kosovo, North Macedonia and Montenegro face the challenge of promoting financial transparency while respecting the cultural significance and historical importance of the Hawala system. This delicate balance requires a nuanced and collaborative approach that engages Hawala operators, communities, financial institutions and international partners (Liargovas and Repousis, 2011).

Challenges and Opportunities

Identifying Challenges in Countering Terrorism and Intelligence Operations Financing: The battle against terrorism has evolved into a multifaceted and global challenge, with financial networks serving as a vital component of extremist organizations' operations. The financing of terrorism and intelligence gathering to track these financial flows have become integral aspects of counterterrorism efforts. However, countering terrorism financing (CTF) and intelligence financing pose several complex challenges that demand continuous adaptation and innovation.

One of the fundamental challenges in CTF is the sheer diversity of financing sources and methods employed by terrorist organizations. These groups have proven adept at adapting to anti-money laundering (AML) and counterterrorism financing regulations by using a variety of channels such as formal banking systems, crypto currencies, trade-based money laundering and charitable organizations (Lodge, 2020). This diversity demands a comprehensive and dynamic approach to monitoring and disrupting these financial flows (Lascaux, 2014).

Additionally, the globalization of financial systems presents hurdles in tracking terrorism financing. Money can move seamlessly across borders, making it difficult to pinpoint the origin and destination of funds. Terrorist groups often exploit this globalized financial system,

moving funds across multiple jurisdictions to evade detection. Effective coordination among international agencies and governments is essential to combat this transnational threat (Đorđević et al., 2018).

Furthermore, the emergence of crypto currencies as a means of raising and transferring funds has further complicated CTF efforts. Crypto currencies offer a level of anonymity and decentralization that makes them attractive to terrorists. Tracking crypto currency transactions requires innovative techniques and tools, as well as cooperation with crypto currency exchanges and blockchain analysis firms.

In the realm of intelligence operations financing, challenges are equally daunting. Intelligence agencies rely on substantial budgets and resources to carry out their missions effectively. Funding must be secured while ensuring the utmost discretion. Additionally, advances in technology have allowed for more sophisticated methods of intelligence gathering and espionage, which can be expensive to develop and maintain.

The issue of human capital is another significant challenge in intelligence financing. Recruiting and retaining skilled personnel is crucial, as intelligence agencies require experts in various fields, including cybersecurity, cryptography and data analysis. Competitive salaries and a conducive work environment are essential to attract and retain top talent in the intelligence field.

Moreover, the balance between privacy and national security is a critical challenge in intelligence operations financing. As governments seek to enhance their intelligence capabilities, they must navigate the delicate balance between safeguarding individual privacy and collecting information necessary for national security. Striking this balance requires legislative frameworks that protect civil liberties while allowing intelligence agencies to operate effectively (Heineman and Nomikos, 2022).

In addition, technological advancements pose both opportunities and challenges in the realm of intelligence operations financing. The proliferation of surveillance technologies, data analytics and artificial intelligence offers new tools for gathering and analysing intelligence. However, these technologies also raise concerns about their ethical use and potential abuses of power, necessitating stringent oversight and accountability mechanisms (Heineman and Nomikos, 2022).

Opportunities for Strengthening Counterterrorism and Counterintelligence Measures: In an increasingly interconnected world where the threat of terrorism remains a persistent concern, there are several critical opportunities for strengthening counterterrorism and counterintelligence measures. These opportunities encompass a broad spectrum of strategies, technologies and international collaborations that can enhance governments' ability to prevent and fight against terrorism. Some of these key avenues for bolstering counterterrorism and counterintelligence efforts are:

1. Enhanced intelligence sharing: Enhanced intelligence sharing in the realm of counterterrorism and counterintelligence is crucial for tackling the Hawala clandestine financial network (Lowe, 2014). Collaborative intelligence sharing among nations and intelligence agencies is vital to identify, track and disrupt these illicit financial flows effectively (Đorđević et al., 2018). By sharing actionable intelligence, such as transaction data, profiles of Hawala operators and emerging trends, countries can better understand the movements of funds within the Hawala system and identify potential links to terrorist financing (Rios. and Insua, 2011; Manjarrez, 2015).

Moreover, cooperation between governments and international organizations can help harmonize legal frameworks and regulatory standards related to Hawala, facilitating information exchange and enforcement across borders (Liashuk and Tsaruk, 2021). Enhancing intelligence sharing is not only a proactive measure to counter terrorism but also an essential aspect of protecting national security and maintaining global stability (Proksik, 2017; Richards, 2018). It enables a collective response to the evolving challenges posed by Hawala and underscores the importance of international collaboration in the fight against terrorism and illicit financial networks (Arsovska, 2019; Bures, 2010; Rahimi, 2021).

2. Advanced data analytics: Advanced data analytics plays a pivotal role in unravelling the intricate web of Hawala transactions and aiding authorities in countering its illicit activities. Hawala, as an informal and clandestine money transfer system, thrives on secrecy and obfuscation (Liashuk and Tsaruk, 2021). To combat this, advanced data analytics techniques offer a powerful tool for uncovering patterns, identifying anomalies and tracing the flow of funds within the Hawala

network (Lowe, 2014). By harnessing big data technologies and machine learning algorithms, law enforcement and intelligence agencies can sift through vast volumes of financial data to identify suspicious transactions, detect money laundering activities and uncover potential links to criminal organizations, including those involved in terrorism (Rios. and Insua, 2011; Lodge, 2020).

Additionally, these analytics tools can help predict future financial movements and trends within the Hawala system, allowing authorities to proactively target key players and disrupt illicit financial flows (Liashuk and Tsaruk, 2021). As Hawala continues to evolve and adapt to evade traditional detection methods, advanced data analytics serves as a crucial instrument in staying one step ahead in the ongoing battle against this clandestine financial network, ultimately enhancing global efforts to combat terrorism, money laundering and other illicit activities that exploit the Hawala system (Lodge, 2020).

3. Cybersecurity measures: Cybersecurity measures are becoming increasingly essential in addressing the vulnerabilities and risks associated with Hawala, an informal money transfer system often exploited for illicit financial activities (Kapsokoli, 2023). As Hawala transactions can now occur electronically through various channels, they are susceptible to cyber threats, including hacking, data breaches and fraud (Lowe, 2014). Implementing robust cybersecurity measures is imperative to protect the integrity of digital Hawala transactions and prevent unauthorized access or manipulation of sensitive financial data. This includes the encryption of communication channels and databases, stringent user authentication protocols, continuous monitoring for suspicious activities and regular security audits (Kapsokoli, 2023).

Furthermore, educating Hawala operators and users about cybersecurity best practices is essential to create a culture of vigilance. By fortifying cybersecurity in the Hawala ecosystem, authorities and financial institutions can not only thwart money laundering and terrorist financing but also safeguard the financial interests of individuals who rely on this system for legitimate transactions, fostering trust and security within the informal financial sector (Lodge, 2020). As Hawala continues to evolve in the digital age, effective cybersecurity measures are paramount in maintaining the integrity of these transactions while curbing their potential misuse for illegal activities (Rahimi, 2021).

4. Countering radicalization online: Countering radicalization online within the context of Hawala presents a multifaceted challenge that demands a proactive and comprehensive approach (Brown, 2011). Extremist groups often exploit the anonymity and unregulated nature of Hawala transactions to fund their activities and facilitate recruitment (Passas, 2017). To address this issue, it's crucial to engage in monitoring and intervention in the digital realm. Online platforms, social media and encrypted messaging services used by radicalized individuals and recruiters must be closely monitored. Collaboration between governments, financial institutions and tech companies is essential to identify and track suspicious financial activities while respecting privacy and civil liberties (Kudlenko, 2019).

In addition, counter-radicalization efforts should include targeted campaigns to raise awareness about the risks associated with extremist financing through Hawala. Empowering communities and individuals to recognize and report signs of radicalization and suspicious financial transactions is key to preventing its spread. In summary, countering radicalization online in the context of Hawala requires a proactive and cooperative approach that combines monitoring, intervention, awareness and community engagement to disrupt the illicit financial flows that sustain extremist activities while safeguarding online freedoms and privacy (Brown, 2011).

5. Community engagement: Community engagement is a vital component in addressing the complexities of Hawala, an informal money transfer system deeply rooted in many regions (Marrero Rocha, 2018). Hawala plays a significant role in the financial lives of communities and it is essential to involve these communities in efforts to combat its potential misuse for illicit activities such as money laundering and terrorism financing (Lodge, 2020). Establishing trust and collaboration with local communities is key to understanding the dynamics of Hawala networks, identifying irregularities and preventing abuse (Kudlenko, 2019). By fostering open dialogues and providing education about the risks associated with illicit Hawala transactions, authorities can empower communities to recognize and report suspicious activities (Rahimi, 2021).

Moreover, community-based initiatives can help legitimize Hawala operations by encouraging compliance with anti-money laundering and counterterrorism financing regulations while preserving the legitimate financial needs of individuals who rely on the system. In essence, community engagement not only strengthens the capacity to combat Hawala-related illicit activities but also builds resilience against extremism, promotes financial inclusion and contributes to more effective and culturally sensitive countermeasures in regions where the Hawala system is prevalent.

6. Soft power and diplomacy: Soft power and diplomacy offer valuable tools in dealing with Hawala, an informal money transfer system often associated with financial opacity and illicit activities. Instead of solely relying on punitive measures, adopting a diplomatic approach that incorporates soft power elements can help build trust, cooperation and compliance within Hawala networks (Rahimi, 2021). Diplomatic efforts can involve engaging with Hawala operators, communities and countries where the system is prevalent, emphasizing dialogue and mutual understanding. By fostering relationships and open channels of communication, authorities can encourage Hawala operators to adopt best practices, implement anti-money laundering and counterterrorism financing regulations voluntarily and report suspicious transactions. Soft power elements, such as cultural exchanges and educational programs, can also be leveraged to promote financial transparency and awareness about the risks associated with Hawala misuse (Müller, 2012).

Furthermore, diplomatic channels can facilitate international cooperation and agreements on regulating Hawala, ensuring consistency in addressing this global issue. In summary, integrating soft power and diplomacy into efforts to deal with Hawala can create an environment of collaboration and compliance rather than confrontation, promoting effective regulation while respecting cultural sensitivities and preserving the essential financial services that the Hawala system provides to communities around the world.

7. International cooperation: International cooperation is indispensable when dealing with the challenges posed by Hawala, an informal money transfer system prevalent in many parts of the world (Rahimi, 2021). Hawala's transnational nature necessitates a united front in tackling its potential misuse for illicit activities such as money

laundering and terrorism financing (Liashuk and Tsaruk, 2021). Effective international cooperation involves sharing intelligence, best practices and regulatory frameworks among nations and international organizations (Rios. and Insua, 2011; Kudlenko, 2019). It also includes promoting standardized approaches to Hawala regulation and compliance, ensuring that one country's efforts do not inadvertently shift illicit activities to another jurisdiction (Gibas-Krzak, 2013). Collaborative efforts can extend to capacity-building programs that assist countries with weaker regulatory frameworks in strengthening their anti-money laundering and counterterrorism financing measures (Jamwal, 2002; Proksik, 2017).

Moreover, promoting dialogue and trust among nations and Hawala operators is crucial in fostering a cooperative environment where illicit financial flows can be detected, disrupted and prevented more effectively. By pooling resources and knowledge, nations can better understand and combat the intricacies of Hawala networks while respecting cultural sensitivities and preserving the legitimate financial services that Hawala provides. Ultimately, international cooperation stands as a linchpin in addressing Hawala's challenges on a global scale, ensuring that efforts to combat its misuse are coordinated, comprehensive and effective across borders (Bures, 2010).

8. Deradicalization and rehabilitation programs: De-radicalization and rehabilitation programs play a pivotal role in dealing with Hawala, as they address not only the financial aspects but also the broader context of extremism and illicit financing (Passas, 2017). Recognizing that Hawala can be exploited by terrorist groups for their funding needs, these programs aim to disengage individuals involved in extremist activities, including those who may misuse Hawala networks (Müller, 2012). By providing individuals with an opportunity to disengage from radical ideologies and reintegrate into society, deradicalization and rehabilitation programs can indirectly disrupt the flow of funds to extremist organizations (Kudlenko, 2019). These programs typically involve counselling, education, vocational training and psychological support to help individuals transition away from extremist beliefs and behaviours (Marrero Rocha, 2018).

Additionally, they can incorporate financial literacy components to raise awareness about the risks of engaging in Hawala transactions for illicit purposes. By addressing both the financial and ideological

dimensions of extremism, deradicalization and rehabilitation programs contribute to a more holistic and sustainable approach to countering the misuse of Hawala. Such programs not only help individuals disentangle from extremist networks but also prevent the recurrence of radicalization and related financial activities, ultimately fostering greater social stability and security.

9. Resilience and preparedness: Resilience and preparedness are critical aspects of dealing with the challenges presented by Hawala, an informal money transfer system with potential vulnerabilities to illicit financial activities. Financial institutions and Hawala operators need to be adequately trained and equipped to identify and report suspicious transactions, thereby fortifying the financial system's ability to withstand attempts at misuse (Rahimi, 2021). Preparedness, on the other hand, entails a proactive stance in anticipating and addressing potential threats within the Hawala system. This involves developing contingency plans and response mechanisms to react swiftly to any signs of illicit financial activity. Law enforcement agencies, in collaboration with financial institutions and regulators, should be well-prepared to investigate and prosecute cases related to terrorism financing through Hawala channels (Bures, 2010).

10. Border security: Border security and travel monitoring are pivotal elements in dealing with Hawala, an informal money transfer system that often transcends national boundaries (Liashuk and Tsaruk, 2021). To effectively combat the misuse of Hawala for illicit purposes, countries must bolster their border security measures to detect and interdict suspicious financial movements. This includes enhancing screening procedures at border crossings and airports, utilizing advanced technologies for detecting large sums of cash and sharing intelligence on potential Hawala networks with neighbouring countries (Jeandesboz, 2020). Additionally, travel monitoring plays a crucial role in tracking individuals involved in Hawala transactions, as they may travel internationally to engage in illicit financial activities (Manjarrez, 2015). Authorities should maintain watch lists of individuals associated with Hawala networks and collaborate with immigration and law enforcement agencies to flag and investigate suspicious travel patterns (Léonard, 2010; Arsovska, 2019). By fortifying border security and travel monitoring efforts, countries can disrupt the flow of funds through

Hawala networks and ensure that individuals involved in illicit financial activities face greater scrutiny and accountability at international entry and exit points (Léonard, 2010). This comprehensive approach is essential in mitigating the risks associated with Hawala and preventing its misuse for activities such as money laundering, terrorism financing and illicit trade (Arsovska, 2019; Jeandesboz, 2020).

Subsequently, the fight against terrorism is an ongoing and complex endeavour that requires multifaceted approaches (Manjarrez, 2015). By capitalizing on opportunities such as advanced intelligence sharing, technology utilization, community engagement and international cooperation, nations can strengthen their counterterrorism measures and work collectively to mitigate the global threat of terrorism (Lowe, 2014). Embracing these opportunities ensures that counterterrorism efforts remain adaptable and effective in the face of evolving threats (Liashuk and Tsaruk, 2021).

Conclusions

The Hawala system in the Western Balkans represents a unique and deeply ingrained facet of the region's socio-economic landscape. Its historical and cultural significance, coupled with its efficiency in facilitating cross-border transactions and remittances, has allowed it to persist despite the challenges posed by formal banking and regulatory systems. However, this informality and lack of oversight have also made the Hawala system vulnerable to exploitation for illicit financial activities, including money laundering, intelligence operations and terrorism financing.

Addressing these challenges requires a balanced and multifaceted approach that acknowledges the legitimate role of the Hawala system while mitigating its potential risks. Regulatory measures, such as anti-money laundering (AML) and counterterrorism financing (CTF) regulations, are essential tools to enhance transparency and oversight. However, harmonizing these regulations across borders and fostering international cooperation remain complex tasks, given the transnational nature of the Hawala system.

Furthermore, Western Balkan communities' engagement and awareness-building efforts play a crucial role in fostering cooperation and trust within Hawala networks. Governments and international

organizations should collaborate with Hawala operators, communities and financial institutions to promote best practices and provide education about the risks associated with the misuse of the system. The goal is to empower individuals to recognize and report suspicious activities while preserving the legitimate financial services that Hawala provides to communities worldwide.

Additionally, research and development initiatives, including advanced data analytics and technological innovations, can offer effective tools for tracking, monitoring and analysing Hawala transactions. These innovations can help authorities gain insights into the flow of funds within Hawala networks and detect patterns indicative of illicit financial activities.

Ultimately, international cooperation is paramount in addressing the Hawala system's challenges comprehensively (Rahimi, 2021). Given its propensity to operate across borders, countries in the Western Balkans must collaborate with their neighbours and international partners to harmonize regulatory standards, share intelligence and coordinate response efforts. Public-private partnerships can also play a pivotal role in encouraging cooperation between financial institutions and Hawala operators.

References:

1. Abbas, T. (2007). "Chapter 1 Introduction: Islamic political radicalism in Western Europe." *Islamic Political Radicalism*, 3-14. https://doi.org/10.1515/9780748630868-003

2. Arsovska, J. (2019). "Western Balkans: Organised crime, political corruption and oligarchs." *Handbook of Organised Crime and Politics*. https://doi.org/10.4337/9781786434579.00015

3. Blockmans, S. (2006). "Western Balkans (Albania, Bosnia-Herzegovina, Croatia, Macedonia and Serbia and Montenegro, including Kosovo)." *The European Union and Its Neighbours*, 315-355. https://doi.org/10.1007/978-90-6704-507-0_10

4. Brown, C. J. (2011). *Countering radicalization: Refocusing responses to violent extremism within the United States*. Naval Postgraduate School.

5. Bures, O. (2010). "Eurojust's fledgling counterterrorism role." *Journal of Contemporary European Research*, 6(2), 236-256. https://doi.org/10.30950/jcer.v6i2.274

6. Çınar, A. E. (2022). "Situating an informal funds transfer system in Islamic Legal Theory: The Origin of Hawala revisited." *Darulfunun Ilahiyat.* https://doi.org/10.26650/di.2022.33.1.1052681

7. Đorđević, V., Klemenc, J. and Kolářová, I. (2018). "Regional Security Cooperation Reinvented: Western Balkans counterterrorism initiative." *European Security*, 27(4), 415-433. https://doi.org/10.1080/09662839.2018.1510831

8. Foertsch, V. (1999). "The role of counterintelligence in Countering Transnational Organized Crime." *Trends in Organized Crime*, 5(2), 123-142. https://doi.org/10.1007/s12117-999-1036-z

9. Gibas-Krzak, D. (2013). "Contemporary terrorism in the Balkans: A real threat to security in Europe." *The Journal of Slavic Military Studies*, 26(2), 203–218. https://doi.org/10.1080/13518046.2013.779861

10. Han, C. R., Leeuw, B. and Nelen, H. (2022). "Mapping Hawala risks around the world: The use of a composite indicator." *Global Crime*, 23(3), 334-363. https://doi.org/10.1080/17440572.2022.2098120

11. Hancock, D. A. (2008). *The olive branch and the hammer: A strategic analysis of hawala in the financial war on terrorism*. Monterey, CA; Naval Postgraduate School.

12. Heineman, N. and Nomikos, I. (2022). "Counterintelligence in the Balkans and eastern & Mediterranean. The counterintelligence methods of transnational groups." *International Scientific Conference STRATEGIES XXI*, 18(1), 141–153. https://doi.org/10.53477/2971-8813-22-17

13. Herbert, S. (2022). *Social Norms, Gender and Serious and Organised Crime in Albania and Kosovo*. https://doi.org/10.19088/k4d.2022.018

14. Hughes, M. (1982). "Terrorism and National Security." *Philosophy*, 57(219), 5-25. https://doi.org/10.1017/s0031819100069515

15. Jamwal, N. S. (2002). "Hawala-the invisible financing system of terrorism." *Strategic Analysis*, 26(2), 181-198. https://doi.org/10.1080/09700160208450038

16. Jeandesboz, J. (2020). "European border policing: Eurosur, knowledge, calculation." *The Policing of Flows*, 92-121. https://doi.org/10.4324/9780429299193-5

17. Kapsokoli, E. (2023). "Cyberterrorism." *Hybrid Threats, Cyberterrorism and Cyberwarfare*, 57–81. https://doi.org/10.1201/9781003314721-4

18. Kudlenko, A. (2019). "The Western Balkan counter-terrorism initiative (WBCTI) and the capability of the EU as a counter-terrorism actor." *Journal of Contemporary European Studies*, 27(4), 503-514. https://doi.org/10.1080/14782804.2019.1652148

19. Lascaux, A. (2014). "Crowding out trust in the informal monetary relationships: The curious case of the Hawala system." *Forum for Social Economics*, 44(1), 87-107. https://doi.org/10.1080/07360932.2014.954250

20. Léonard, S. (2010). "EU border security and migration into the European Union: FRONTEX and securitisation through practices." *European Security*, 19(2), 231–254. https://doi.org/10.1080/09662839.2010.526937

21. Liargovas, P. and Repousis, S. (2011). "Underground banking or Hawala and Greece-Albania remittance corridor." *Journal of Money Laundering Control*, 14(4), 313–323. https://doi.org/10.1108/13685201111173794

22. Liashuk, R. and Tsaruk, A. (2021). "Experience of information and analytical activities in the field of Border Protection of the European Union." *Proceedings of the International Conference on Economics, Law and Education Research* (ELER 2021). ttps://doi.org/10.2991/aebmr.k.210320.032

23. Lodge, H. D. (2020). *Anti-money laundering. Blackstone's Guide to The Sanctions and Anti-Money Laundering Act*. https://doi.org/10.1093/oso/9780198844778.003.0013

24. Lowe, D. (2014). "Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty." *Terrorism and Political Violence*, 28(4), 653-673. https://doi.org/10.1080/09546553.2014.918880

25. Manjarrez, V. M. (2015). "Border Security: Defining it is the Real Challenge." *Journal of Homeland Security and Emergency Management*, 12(4), 793–800. https://doi.org/10.1515/jhsem-2015-0052

26. Marrero Rocha, I. (2018). "The European Union's foreign 'terrorist' fighters." *Jihadism, Foreign Fighters and Radicalization in the EU*, 44-63. https://doi.org/10.4324/9780429468506-4

27. Müller, S. R. (2012). *Hawala: An informal payment system and its use to finance terrorism*. AV Akademikerverlag.

28. Passas, Nikos. (2017). "Demystifying hawala: A look into its social organization and mechanics." *Transnational Financial Crime*, 171-188. https://doi.org/10.4324/9781315084572-12

29. Proksik, J. J. (2017). "Eulex and the fight against organised crime in Kosovo: What's the record?" *Trends in Organized Crime*, 21(4), 401-425. https://doi.org/10.1007/s12117-017-9321-8

30. Rahimi, H. (2021). "How to create better hawala regulations: A case study of hawala regulations in Afghanistan." *Crime, Law and Social Change*, 76(2), 131–148. https://doi.org/10.1007/s10611-021-09959-w

31. Richards, J. (2018). *Intelligence and counterterrorism*. Routledge Handbook of Terrorism and Counterterrorism, 395-405. https://doi.org/10.4324/9781315744636-34

32. Rios, J. and Insua, D. R. (2011). "Adversarial Risk Analysis for Counterterrorism Modelling." *Risk Analysis*, 32(5), 894-915. https://doi.org/10.1111/j.1539-6924.2011.01713.x

LIVE TERROR A NEW WAY/MODEL OF ONLINE RADICALIZATION?

Alina-Bianca COSCA*

Abstract:
With the exponential development of the virtual environment and social networks, radical elements have managed to promote and disseminate their radical ideas, in less time, to a wider and more diversified audience than in the past. This aspect has caused a shift of radicalization processes from the offline environment to the online environment, turning online radicalization into one of the biggest security challenges. This paper aims to (1) provide an insight into the hypothesis according to which the live-streaming of terrorist attacks in recent years could become a new radicalization mechanism, perhaps generating a new trend and (2) identify the elements and dynamics that determine attackers to use live-stream platforms at the time of the terrorist attack. The article proposes an analysis of the current theoretical framework that combines the brief analysis of the main models of online radicalization, highlighting the elements that could underlie a new radicalization model focused on live-stream/copycat terrorist attacks. In this article we aim to answer the following research question: can live-streaming represent a new mechanism of radicalization?

Keywords: *radicalization, live-streaming, propaganda, violent extremism.*

Introduction

We are almost constantly connected to a virtual reality, which is increasingly gaining ground at the expense of everyday reality. The facilities offered by the online environment together with the live-streaming services of well-known platforms such as Facebook Live, Periscope, Twitch, Instagram favoured the significant and varied absorption of virtual content by Internet users.

The past era when the messages of terrorist organizations hardly managed to penetrate the borders of Western states is totally in contrast

* PhD student, ANIMV Bucharest, email: cosca-voin.bianca@animv.eu.

with the current capabilities of terrorist organizations that, with the help of digital technology, have revolutionized the concepts of propaganda and radicalization, managing to be one click away from the users of the virtual environment. Thus, with the development and benefits brought by the online environment, terrorist elements have transformed the virtual environment into a key tool in propaganda and radicalization actions. Moreover, with the advent of live-streaming platforms, the radicalization process and modern propaganda mechanisms have been resized.

Although scientific evidence proving the hypothesis that the Internet plays a direct role in the radicalisation process continues to be limited, and existing studies of online radicalisation have focused predominantly on media content that disseminates opinions, the online environment remains an important factor of radicalisation processes, insufficiently studied in relation to the influence it can have on individuals by promoting attitudes and behaviours that generate violence.

With the exponential development of the virtual environment and social networks, radical elements have managed to promote and disseminate their radical ideas, faster, to a larger and more diversified audience than in the past. This aspect has led to a reorientation of radicalization processes carried out in an offline environment to an online environment, turning online radicalization into one of the biggest security challenges.

This paper aims to (1) provide a perspective on the hypothesis according to which the live-streaming of terrorist attacks in recent years could become a new radicalization mechanism, generating a new trend and (2) identify the elements and dynamics that determine the attackers to use live-stream platforms when committing terrorist attacks.

This article proposes an analysis of the current theoretical framework that combines the brief analysis of two main models of online radicalization, highlighting the elements that could underlie a new

radicalization model focused on live-stream[1]/ copycat[2] terrorist attacks. In this context, one of the key questions we will try to answer is: what motivates attackers to transmit a terrorist attack in real time, through live-stream platforms?

Theorizing Online Radicalization

Existing scientific research on the role that virtual environment plays in the radicalization processes and on how the interaction between individuals and online extremist content influences radicalization are most often theoretical, descriptive and insufficient (von Behr et al., 2013; Bastug, Douai & Akca, 2018, Mølmen & Ravndal, 2021; Gill & Corner, 2017). Empirical research in online radicalisation highlights that the path to violent, terrorist actions is complex and relies on both offline and online triggers that play an interconnected role (Gill et al., 2019, 2017; Koehler, 2014; von Behr et al., 2013), the online environment representing only one dimension in the process whose effect needs to be analysed and understood in a larger context (Ines von Behr, 2013).

In order to understand online radicalization and beyond, we need to understand both the needs, impulses, forms of manifestation that led to and determined an individual to radicalize and commit a terrorist attack, as well as the mechanisms and virtual support that facilitated and accelerated the radicalization process. Like the concept of classical radicalisation, online radicalisation is not explicitly defined, there is no agreement on what it is and how it takes place, which gives rise to interpretations (Meleagrou-Hitchens & Kaderbhai, 2017; Gill, 2015; Herath & Whittaker, 2023) addressing issues such as: where does radicalization actually occur, what is the interplay of the offline and online environment, etc.?

The current research starts from current descriptions and models of radicalization that also focus on the role of online environment plays in initiating, sustaining and carrying out the process of radicalization.

[1] Streaming is a technological phenomenon, made up of platforms that pump non-stop information to devices connected to the internet, so users have real-time access to content without having to download the desired material.

[2] Someone who is influenced by someone else and does or says exactly the same as them.

Individuals interact with and are exposed to different types of content in the virtual environment, adopt beliefs that legitimize violence, and shape these beliefs to the point where they are translated into violent actions.

Current models of online radicalisation

In the literature, there are various models of online radicalisation, among them is that of Bastug, Douai and Akca. This model presents a mechanism that can lead a person to commit a terrorist act in four steps, targeting the accessibility and duplication of radical content in the online environment, and the susceptibility and predisposition of some people to resonate with radical content. Another model is the radicalisation factor model (RFM) of Babak Akhgar and Douglas Wells (2019) which aims to integrate into a common framework the causal factors of online radicalisation process and the mechanisms by which an individual gets in contact with extremist ideas and can reproduce them. A third model was proposed by Guri Nordtorp Mølmen and Jacob Aasland Ravndal (2023) which emphasizes the causal mechanisms and modalities that fuel and connect radical ideas online with violent actions, highlighting six mechanisms, namely compensation, isolation, facilitation, acceleration, echo effect and triggering violent action.

Given that the objective of the research is to identify how the live-stream contributes to the radicalization process, I will analyse the models of radicalization highlighted by G. Weimann and Von Knop (2008) and Loo Seng Neo (2019). These two models of radicalization emphasize both online radicalization mechanisms and their interpenetration with radicalization factors, aspects that can be a key element in shaping a radicalization model related to live-stream terrorist attacks and copycat effect.

The model of G. Weimann and Von Knop

The online radicalization model of G. Weimann and Von Knop (2008) is based on the search stage, in which individuals try to fulfil their own needs, motivations (spiritual, psychological, social, belonging, recognition) by searching and identifying answers in the online environment that resonate with them and their needs. This phase is

followed by the stage of seduction or persuasion, considered to be the most important, because, within it, users are no longer passive but become active in the online environment, being attracted by the radical ideologies. Once seduced, individuals enter the captivity stage where they begin to access forums, blogs, chat rooms, echo-chambers, being attracted by seductive propaganda, becoming part of the online radical communities. Most elements in the process of online radicalization stop at this stage and do not move to the last phase, meaning the operative/ actional one, which involves familiarizing users with various activities prior to terrorist action.

The Model Reflection, Exploration, Connection, Resolution, Operational ("RECRO")

Loo Seng Neo's "RECRO" model (2019) is a five-step model of how the person and the characteristics of online platforms complement and influence each other during the radicalisation process. The five stages of the model are: reflection phase (details the triggers, needs and vulnerabilities of an individual, developing interest and receptivity to alternative systems to meet their needs); the exploration phase (represents the period when the individual begins to make sense of online information presented by violent extremists); the connection phase (refers to the interaction, the influence of like-minded individuals and the online community regarding the new worldview perceived by the individual); the resolution phase (refers to the individual's impulse to translate their radical beliefs into action); the operational phase (is the period during which the individual can commit acts of violence to achieve the intended goals).

The chance that a person will become receptive to radical narratives depends on how these online narratives relate to their life experiences (Weimann and von Knop, 2008). Also, the developed receptivity to alternative belief systems depends on the triggers, needs, and vulnerabilities of the reflection phase. Thus, the first two phases take place in a parallel rather than sequential manner, and cannot be separated in reality (Borum, 2011). Following the exploration phase, the radicalized individuals initiate connections with elements that share their visions, creating online communities in echo chambers, based on

similar interests and ideas that allow the individuals to find support and strengthen their new worldview (Bowman-Grieve, 2013; Thomas, Mcgarty & Louis, 2014). Following the resolution phase, the need to act violently may lead the individual to dedicate more time and resources to contribute to the cause. Wilner and Dubouloz (2011) highlight that violent behaviour is a product of individuals' newly acquired value system, in which revenge is not only justified, but expected.

Apparently these radicalization models are different, but in essence they are complementary, having a series of common aspects: (1) the motivational element composed of both pull (feeling of dissatisfaction, unfulfillment, etc.) and push factors that can serve as incentives (acquired status, importance within the group, hero image, etc.); (2) the need to identify responses or meet social needs; (3) the individuals' gradual decision to engage in terrorist actions, (4) the seduction mechanism offered by the virtual environment; (5) a high degree of similarity, at least in terms of the trigger elements of radicalization, namely a feeling, an experience considered unfair, unjust by the individual and transformed into hatred towards a real or fancied culprit is found in the models of Babak Akhgar and Douglas Wells, Loo Seng Neo.

Although in the last years there has been an increase in online radicalization associated with extremist/radical propaganda created by individuals who broadcast their own terrorist attacks live, current models of online radicalization tend to focus mostly, if not exclusively, on the individual consuming virtual radical propaganda and less or not at all on his role as a prosumer, both producer and consumer of radical materials and on the fact that this dual role can constitute a mechanism of online radicalization.

Given the fact that the live-streaming of terrorist actions allows: (1) users to access real time extremist videos content, that is engaging, captivating; (2) connection to real emotions, feelings from the moment of the action carried out; (3) a much faster identification with similar visions and behaviour; (4) a spread of responsibility to duplicate the same type, kind of behaviour and action in the name of an ideology (be it right-wing or Islamist); (5) the considerable narrowing of the distance between the viewer/consumer/spectator and the victim, bringing him/her to the forefront, correlated with the fact that at least the far-right

perpetrators in the last six years have inspired each other in the process of radicalization and committing terrorist actions, we can hypothesize that live-streaming can represent a mechanism for accelerating the radicalisation processes. To verify this hypothesis, I will analyse a series of attacks that have been live-streamed and identify the ways in which the perpetrators have influenced each other.

Terrorists' live-streaming attacks

In September 1972, television broadcasts from around the world, present at the Olympic Games in Munich/ Germany, captured live the terrorist attack committed by members of the Palestinian group "Black September". Then, in September 2001, TVs broadcast live the moment when the second plane hijacked by members of the terrorist organization Al Qaeda hit World Trade Centre. In retrospect, it is undeniable that the two terrorist organizations relied on the media impact, but at that time these two attacks could not be considered "live-stream attack" type of action.

Technology, the latest high-tech capabilities and online services have become essential for the survival of any extremist/terrorist organization. Thus, in the last decade we notice that terrorist organizations have created their own press agencies, online publications, radio stations, social media channels, vital tools for propaganda and recruitment activities, trying to keep pace with the restrictive measures implemented at the level of Western states to prevent and combat extremist propaganda and radicalization.

In addition to all these elements, in recent years a new propaganda method has been developed. It is much more brutal, more direct, more personal, and assigns the bomber a triple role: that of main actor focusing on the live transmission of the terrorist attack, producer of terrorist propaganda and model of inspiration for future attackers. Both far-right and Islamist terrorist elements have made steady strides in using body-worn video (BWV) cameras and stream channels for live, real-time transmission of terrorist attacks and elements inside the attack.

The pioneers of these methods of propaganda and radicalization are Al Shabaab, the ISIS-affiliated terrorist group that transmitted in real time, on Twitter, information, images, details from the attack on

September 21, 2013 at the Westgate Mall in Nairobi, Kenya. Subsequently, Mohammed Merah, the perpetrator of the March 2012 terrorist attacks in Montauban and Toulouse, France, used a GoPro camera attached to his body to film and promote the attack, the video being sent to the Al Jazeera news agency, which decided not to make it public.

The one who managed to broadcast live the attack is Larossi Abballa, the author of the attack in Magnanville/France. On the evening of June 13, 2016, he stabbed to death a policeman, breaking into his house and killing his wife with the same weapon. The bomber used the Facebook app to live-stream a 13-minute clip from the scene of the attack and declare his loyalty to ISIS. Following the attack, ISIS news agency uploaded an edited version of the live-streamed video to YouTube, which garnered more than 9.000 views.

Another promoter of Islamist ideology is Abdoulakh Anzorov, the author of the October 16, 2020 attack in Paris, France. He beheaded history teacher Samuel Paty, filmed the attack, and the images became viral, being shared on Telegram.

Among the Islamist bombers who intended to broadcast live the terrorist attacks committed, but for various reasons (mainly technical) failed to complete their approach are: Mehdi Nemmouche, the bomber at the Jewish Museum in Brussels/Belgium, on May 24, 2014, who was carrying a portable video camera with which he intended to broadcast the attack live. After the attack, a video was found in which Mehdi Nemmouche expressed regret for not being able to successfully transmit the attack. Amedy Coulibaly, the perpetrator of the January 2015 attack on a Jewish hypermarket in Paris, also used a BWV camera during the siege. Although there is no clear information on whether the images went viral on jihadist platforms, according to witnesses, Amedy Coulibaly downloaded the images from the siege from the camera's memory card to a laptop.

Also, in December 2023, a 22-year-old British man was convicted of planning to commit a gun attack on a Christian preacher at Hyde Park's Speakers' Corner, a venue famous in London for attracting propagandists and influential religious leaders. The possible perpetrator downloaded al-Qaeda publications and other extremist material, saying he intended to carry a video camera to live-stream the attack.

Another example is that of US citizen Munir Abdulkader who aimed to kill military personnel and execute/behead them live, the materials being intended for ISIS propaganda. Unlike terrorist attacks committed by followers of Islamist ideology about which we cannot highlight whether they clearly and directly caused other individuals to commit terrorist actions, live-stream terrorist attacks committed by radical elements, promoters of right-wing ideology inspired and determined other radical followers to commit terrorist actions.

One of the far-right bombers who live-streamed a terrorist attack, becoming an inspiration for his successors is Brenton Tarrant, the perpetrator of the attack on mosques in Christchurch/ New Zealand, on March 15, 2019. He live-streamed the attack on various online platforms, including Facebook, for 17 minutes. Within 24 hours of the attack, Facebook removed 1.5 million videos of the massacre at the two mosques in Christchurch and blocked 1.2 million clips from uploading, with 300.000 videos existing on Facebook at any given time. Prior to the attack, Brenton Tarrant promoted a 74-page manifesto online titled "The Great Replacement" that drew similarities to the manifesto posted by Anders Behring Breivik, the 2011 bomber. Breivik did not live-stream on purpose, the television stations broadcast the events on the island of Utøya (Norway), which led to his followers having access to these videos.

In October 2019, Stephan Balliet live-streamed on Twitch, 35 minutes of the attack committed at a synagogue in Halle/Germany, as part of the Balliet video promoting anti-Semitic ideas. Brenton Tarrant was the artisan who inspired Hugo Jackson, the perpetrator of the attack on the Källeberg School in Eslov/Sweden on August 19, 2021. Jackson live-streamed the attack on Twitch for over 9 minutes, using his phone as a makeshift BWV device mounted on his helmet. When starting the live-stream, the 15-year-old quoted Brenton Tarrant as urging followers to subscribe to the PewDiePie YouTube channel.

Also, 18-year-old Payton Gendron, the Buffalo/New York bomber on May 14, 2022 live-streamed part of the attack on video streaming platform Twitch. Inspired by Brenton Tarrant, Payton Gendron posted an online diary of over 700 pages and a manifesto containing 180 pages, part of which was quoted, plagiarized from the one promoted by Brenton Tarrant, in which he explains his motives and beliefs for committing a terrorist attack. Although the live-stream was watched by only

22 people, being removed by Twitch within two minutes of its launch, the copies made were widely posted online (Twitter, Instagram, Reddit), attracting millions of views on Facebook and other platforms in just a few hours. Thus, a copy uploaded to an alternative streaming site was viewed more than three million times before its removal. Also, the existing link on Facebook was deleted after more than ten hours, during which it was shared more than 46,000 times within the platform. 30 minutes before live-streaming began, Payton issued a series of invitations to Discord users, containing access to the chat room where his logs were posted and a series of online messages containing the Twitch live-stream link he used to broadcast the attack. Chat logs indicated that the attack was originally planned to take place on March 15 so that the perpetrator could commemorate the anniversary of the Christchurch mosque shootings, having been postponed because the bomber was diagnosed with COVID-19.

From Zero to Hero: Explore the Role Live-streaming Play in Radicalization Process

The online environment/social networks play an active role in disseminating their own radical experiences and their increasing consumption by users, which creates a loop effect, respectively the individual initially consuming online propaganda becomes its producer inspiring other consumers who will later become those who produce extremist materials. D. Koehler (2014) argues that the benefits offered by the virtual environment, such as anonymity, space without constraints, efficient communication, unlimited access to information, visibility, determine vulnerable elements, in the process of radicalization, to want to shape and promote a new version of themselves (a better me but in a wrong and negative way).

According to the online radicalization models of L. S. Neo and G. Weimann and Von Knop, vulnerable people, with background elements that make them prone to radicalization, initially go through a stage called reflection or search, in which they aim to identify an alternative to meet certain needs such as validation, integration, recognition at community level, etc. Analysing the background elements and the journey of both Tarrant Brenton and Payton Gendron until the terrorist attacks were

committed, it indicates that the online environment represented an alternative, a solution to the experiences and social life experienced by the two people.

Tarrant Brenton grew up in a single-parent family, as his parents divorced when he was young. According to his mother, Shaton Tarrant, he was traumatized by the divorce, the loss of home in a fire and the death of his father. Following his parents' separation, Brenton Tarrant was characterized as a person suffering from social anxiety, being bullied by both his stepfather and schoolmates. Tarrant Brenton became attracted to video games at the age of seven, during the period when he and his mother were exposed to verbal and physical violence. He was mainly involved in first-person shooter games and massive multiplayer online role-playing games, and at 14 he began using the platform "4chan3", later accessed by Gendron Payton as well.

In 2007, when Tarrant Brenton was 17 years old, his father was diagnosed with lung cancer, and in 2010, he committed suicide, Tarrant Brenton being the one who discovered it. The diagnosis and subsequent death of his father exacerbated his social anxiety and stress (according to the report published by the Royal Commission of inquiry into the terrorist attack on Christchurch Mosque), and he was further drawn to ultra-nationalist messages and hatred of Muslim immigrants in Western countries.

Along the same line, Gendron Payton, according to his classmates' description, was a socially awkward, withdrawn boy. According to the self-description in his manifesto, Gendron Payton was a pure, white man whose experiences and personal life were worthless, and he was looking for a way to protect and serve his community, culture, and race. Mostly connected to the reality of online streaming games, Gendron Payton was interested in and fascinated by anything that could attract the attention of his colleagues and of the people around him, such as firearms.

The stage of seduction, persuasion or exploration in the case of the two attackers is highlighted by the ideological stages taken, especially

[3] Anonymous English-language website known as an online subculture hub with an influential community in promoting movements such as Anonymous and alt-right but also in creating and publicizing memes such as lolcats, Rickrolling, rage comics, wojaks, Pepe the Frog.

by Gendron Payton who initially identified himself as a promoter of left-wing ideology, later promoting anti-Semitic, neo-Nazi and far-right ideas. Payton said he adopted these ideological positions after visiting a number of websites and discussion forums, including 4chan.

The phases of captivity, resolution and connection are highlighted in Gendron Payton's case by the support he expressed in his diary to his predecessors Anders Behring Breivik and Brenton Tarrant, constantly mentioning that he was inspired by the latter. This is also apparent from the fact that 57% of his manifesto is copied from the one promoted by Brenton Tarrant. Gendron Payton's desire to put his visions and ideas into practice is also evidenced by planning the attack months in advance, posting in his diary that he entered the store where he committed the attack several times, and came to know its daily operations. Both Brenton Tarrant and Gendron Payton have reached the final stage of online radicalization, respectively operational, committing terrorist attacks.

P. Neuman (2013), M. Sageman (2009), T. Psyszczynski (2009), J. Whittaker (2019) highlight the fact that online radicalization is based on a series of dynamics that involve creating a sense of importance of one's own death, self-sacrifice, learning and normalizing deviant behaviours (with the help of echo chambers), creating the effect of online disinhibition and hyperbolized virtual image. The idealized and zealous individuals online are actually idealized versions of the real persons.

Far-right attackers and not only, in recent years, invoke the online environment as the starting point in their journeys towards radicalization, and the combination of online diaries and live transmission of terrorist attacks they commit represent not only a window into the radicalization process undergone, but also a mechanism to inspire and disseminate to a wider audience the attacker's view.

Analysing the typology of attackers who have committed live terrorist attacks in recent years, it is evident that their profile is predominantly that of vulnerable, socially isolated people who feel uncomfortable in society (as Payton Gendron said about himself in the journals promoted online), looking for a validation from society and the community to which they belong (e.g. Payton Gendron mentioning that the live broadcast of the attack will make those who watch him to applaud him), who were radicalized by consuming propaganda online.

The option of committing a terrorist attack live brings the attacker to the forefront, giving him the opportunity to get out of anonymity, to differentiate himself from others, to give birth to a trend, to become a model, an influencer for other people.

Also, live-stream attacks place the attackers in the foreground, in the role of hero in the vision of other followers of the promoted ideology, but also of propaganda creator, giving them the possibility to personalize and brutalize the attack and create a dynamic propaganda.

Conclusions

Attempts in recent years to broadcast a terrorist attack live highlight the possibility of developing a new way of acting and a new method of radicalisation and propaganda. The authenticity of the live content broadcast at the time of the terrorist attack generates maximum impact on the audience, but also a serial action, an act of violence inspiring the next act of violence as Payton Gendron was inspired by Brenton Tarrant and Tarrant by Anders Breivik.

Personal, planned live-streams with a well-defined purpose or just driven by the current trend of going viral could represent a mutation in the modus operandi of extremist/ jihadist elements.

If when we refer to the live-stream attacks committed in recent years by the promoters of radical right-wing ideology we can conclude that this way of promotion was a method of inspiration for other people who committed terrorist attacks. As far as the Islamist bombers who broadcast the attacks live are concerned, there are currently no studies to attest, to validate that their actions have inspired, radicalized and led other individuals to commit terrorist attacks, perpetuating this course of action.

The purpose of this article, to provide insight into the hypothesis according to which the live transmission of terrorist attacks in recent years could become a new mechanism of radicalization, has been partially achieved. The lack of clear studies and data meant to help shape a response to how the live-stream of Islamist terrorist attacks and the copycat effect inspired or no other followers in carrying out terrorist actions makes this working hypothesis a subject of open study.

However, given the fact that terrorist attacks committed live by elements promoting radical right-wing ideology have managed to inspire and determine followers to continue this mode of action, it is not excluded that in the future live-streaming terrorist attacks will become a trend, the visibility, dynamics, projection of an image of power and control of the bomber, the reduced distance between the attackers and the victim representing primary elements in choosing this mode of action.

References:

1. Akhgar, B., Wells, D., & Blanco, J. M. (Eds.). (2019). "Investigating Radicalization Trends: Case Studies in Europe and Asia." Springer Nature.

2. Bastug, M. F., Douai, A., & Akca, D. (2020). "Exploring the 'demand side' of online radicalization: Evidence from the Canadian context." *Studies in Conflict & Terrorism*, 43(7), 616-637.

3. Bayerl, P. S., Staniforth, A., Akhgar, B., Brewster, B., & Johnson, K. (2014). "A framework for the investigation and modelling of online radicalization and the identification of radicalized individuals." *Emerging trends in ICT security* (pp. 539-547).

4. Bertram, S., & Ellison, K. (2014). "Sub Saharan African terrorist groups' use of the internet." *Journal of Terrorism Research*.

5. Bernhardt, J. M., Mays, D., Eroğlu, D., & Daniel, K. L. (2009). "New communication channels: changing the nature of customer engagement." *Social Marketing Quarterly*, 15(1_suppl), 7-15.

6. Brachman, J. M. and Levine, A. N. (2011). "You Too Can Be Awlaki." *The Fletcher Forum of World Affairs*, 35(1), pp. 25–46.

7. Borum, R. (2011). "Rethinking radicalization." *Journal of Strategic Security*, 4(4), 1-6.

8. Browning K. (2022). *After Buffalo Shooting Video Spreads, Social Platforms Face Questions*. https://www.nytimes.com/2022/05/15/business/buffalo-shooting-social-media.html

9. Condon, B., Hill M. (2022), *Buffalo suspect: lonely, isolated, with a troubling sign.* https://apnews.com/article/buffalo-supermarket-shooting-government-and-politics-race-ethnicity-978bddfec22344fe73e30ca34f491784

10. Collins, B. (2022), *The Buffalo supermarket shooting suspect allegedly posted an apparent manifesto repeatedly citing 'great replacement' theory*.

https://www.nbcnews.com/news/us-news/buffalo-supermarket-shooting-suspect-posted-apparent-manifesto-repeate-rcna28889

11. EUROPOL, *European Union Terrorism Situation and Trend Report 2016*. https://www.europol.europa.eu/activities-services/main-reports/european-unionterrorism- situation-and-trend-report-te-sat-2016.

12. Elamroussi A., Moshtaghian A., Frehse R. (2022). *Buffalo suspect's posts about attack plans could be seen online 30 minutes before mass shooting*. https://edition.cnn.com/2022/05/18/us/buffalo-supermarket-shooting-wednesday/index.html

13. Fassrainer V. (2020). *Tweeting Terror Live Al-Shabaab's Use of Twitter during the Westgate Attack and Implications for Counterterrorism Communications*. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2020/Fassrainer-Tweet-Terror/;

14. Ghosh, S. (2019), *Facebook, facing huge criticism over live streaming, says it removed 1.5 million videos of the New Zealand shooting in 24 hours*. https://www.businessinsider.com/facebook-removed-15-million-videos-of-the-new-zealand-mosque-shootings-in-24-hours-2019-3

15. Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). "Terrorist use of the Internet by the numbers: Quantifying behaviours, patterns, and processes." *Criminology & Public Policy*, 16(1), 99-117.

16. Gill, P., Corner, E., Thornton, A., & Conway, M. (2015). *What are the roles of the Internet in terrorism? Measuring online behaviours of convicted UK terrorists*.

17. Koehler, D. (2014). "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, (1), pp. 116–134.

18. Lupu, Y., Sear, R., Velásquez, N., Leahy, R., Restrepo, N. J., Goldberg, B., & Johnson, N. F. (2023). *Offline events and online hate*. PLoS one, 18(1), e0278511.

19. Mac R. (2022). *Gunman's Video Surfaces, With Ads, on Facebook*.

20. Macdonald, S., & Whittaker, J. (2019). *Online radicalization: Contested terms and conceptual clarity*. CRC Press.

21. McConnell, T. (2015). *Close your eyes and pretend to be dead. Foreign Policy*, 20.

22. McMahton L. Vallance C. (2022). *Social platforms' Buffalo shooting response called inadequate*. https://www.bbc.com/news/technology-61466049

23. Meleagrou-Hitchens, A., Hughes, S. and Clifford, B. (2020). *Homegrown: ISIS in America.* London: I. B. Tauris.

24. Meleagrou-Hitchens, A. and Kaderbhai, N. (2017) *Research Perspectives on Online Radicalisation: A Literature Review, 2006-2016*, Vox Pol.

25. Neo, L. S. (2019). *An Internet-mediated pathway for online radicalisation: RECRO. In Violent Extremism: Breakthroughs in Research and Practice* (pp. 62-89). IGI Global.

26. Neo, L. S. (2016). "An Internet-Mediated Pathway for Online Radicalisation: RECRO," in: Khader, M. (Ed.) Combating Violent Extremism and Radicalization in the Digital Era. Hershey, PA: Information Science Reference, pp. 197–224.

27. Neumann, P. (2013). *Options and Strategies for Countering Online Radicalization in the United States. Studies in Conflict & Terrorism*, 36(6), pp. 431–459.

28. Pearlman L. (2012). "Tweeting to Win: Al-Shabaab's Strategic Use of Microblogging," *Yale Review of International Studies*, http://yris.yira.org/essays/837.

29. Pozzoli M. (2024). *POV: Wearable Cameras and the Gamification of Lone-Actor Terrorist Violence*. https://gnet-research.org/2024/02/28/pov-wearable-cameras-and-the-gamification-of-lone-actor-terrorist-violence/

30. Pyszczynski, T. et al. (2006). "Mortality Salience, Martyrdom, and Military Might: The Great Satan Versus the Axis of Evil." *Personality and Social Psychology Bulletin*, 32(4), pp. 525–537.

31. Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019.

32. Rubin, A. J., & Blaise, L. (2016). "Killing Twice for ISIS and Saying So Live on Facebook." *The New York Times*, 14.

33. Sageman, M. (2008). "The Next Generation of Terror," *Foreign Policy*, (March/April), pp. 36–42.

34. Sageman, M. (2011). *Leaderless jihad: Terror networks in the twenty-first century*. University of Pennsylvania Press.

35. Sanchez R. (2016). *Ex-Army recruit pleads guilty to trying to bomb Fort Riley in Kansas*, https://edition.cnn.com/2016/02/03/us/fort-riley-kansas-bomb-attempt-plea/index.html

36. Sardarizadeh S. (2022). *Buffalo shooting: How far-right killers are radicalized online*. https://www.bbc.com/news/blogs-trending-61460468

37. Schuurman, B., & Taylor, M. (2018). "Reconsidering radicalization: Fanaticism and the link between ideas and violence." *Perspectives on Terrorism*, 12(1), 3-22.

38. Spears, R. et al. (2002). "Computer-Mediated Communication as a Channel for Social Resistance: The Strategic Side of SIDE," *Small Group Research*, 33, pp. 555–574.

39. Suler, J. (2004). "The Online Disinhibition effect," *CyberPsychology & Behaviour*, 7(3), pp. 321–326.

40. Reding, A., von Behr, I., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*.

41. Torok, R. (2013). "Developing an explanatory model for the process of online radicalisation and terrorism." *Security Informatics*, 2, 1-10.

42. U.S. Department of Justice (2016). *Ohio Man Sentenced to 20 Years in Prison for Plot to Attack U.S. Government Officers*. https://www.justice.gov/opa/pr/ohio-man-sentenced-20-years-prison-plot-attack-us-government-officers

43. Weimann, G., & Jost, J. (2015). "New terrorism and new media." *Zeitschrift für Außen-und Sicherheitspolitik*, 8, 369-388.

44. Weimann, G. and Von Knop, K. (2008). *Applying the Notion of Noise to Countering Online Terrorism.*

45. Whittaker, J. (2022). "Rethinking online radicalization." *Perspectives on Terrorism*, 16(4), 27-40.

Websites:

https://christchurchattack.royalcommission.nz/the-report/firearms-licensing/the-firearms-licensing-process/
https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya;
https://www.adl.org/resources/blog/footage-buffalo-attack-spread-quickly-across-platforms-has-been-online-days.
https://www.counterextremism.com/extremists/brenton-tarrant

HISTORY AND MEMORY IN INTELLIGENCE

THE ROOTS AND INSTRUMENTS OF RUSSIA'S PROPAGANDA CAMPAIGN

Marius-Răzvan PREDOANĂ*
Ana-Rodica STĂICULESCU*
Bianca-Elena STAN*

Abstract:
In the contemporary era, the Russian Federation conducts a robust global propaganda campaign, with the Kremlin's information warfare operations serving as a crucial component of its foreign policy. Online social media platforms are key battlegrounds where Russia asserts control. The primary aim of Kremlin propaganda is to reinforce the foreign policy objectives of the Russian Federation, both domestically and internationally, by disseminating pertinent information targeted at Russian citizens abroad. The purpose of the article is to present Russian propaganda as a means used by the Russian Federation in promoting its interests.

As we shall mention in the article, various sources are utilized by the Russian Federation to convey propaganda messages to foreign audiences. Notably, certain media outlets such as Russia Today or Sputnik were not designed for the domestic Russian audience but rather for external influence. In addition to official channels, numerous websites spread Russian propaganda, some purportedly operated directly by the government and others managed by bots.

Keywords*: Russian propaganda, communism, disinformation, influence, manipulation.*

Introduction in Russian propaganda - Historical roots

One of Vladimir Putin's ambitions is for the Russian Federation to have influence over the old territories of the Russian Empire. To achieve

* PhD Student, University of Bucharest, email: marius-razvan.predoana@s.unibuc.ro.
* Professor, "Ovidius" University of Constanta, email: ana.staiculescu@unibuc.ro.
* PhD Student, University of Bucharest, email: bianca-elena.stan@s.unibuc.ro.

this goal, the Kremlin political class together with the regime's ideologues officially launched the concept of "Russkiy mir" (tr. Russian World), starting in 2007. Subsequently, the ideology of "Russkiy mir" was conceptualized, developed and promoted insistently through information campaigns and PR companies both among Russian speakers from the domestic environment and from outside the Russian state through television shows, mass media, but also through scientific literature, especially historical, political, and economic. Concretely, this concept, which consists in creating a "Russian World," is used for ideological purposes by both Russian politicians and Russian propaganda, to create a union of Russians everywhere, but especially to "create an alternative to the Soviet Union" (Sazonov & Müür, 2015).

A multitude of myths, ideas, stories, historical phenomena originating in the 18th, 19th, 20th centuries (such as Holy Russia, Russian soul, Russian World) are mainly used by the Russian propaganda machine in an innovative form, to convince the audience it addresses. For example, a variety of myths and historical stories from the pre-1917 period of the Russian Empire have resurfaced and been combined with other narratives of Soviet origin. The concept of Pax Russica was introduced by the Bolsheviks, who, as early as 1920 (Voicu, 2018), had established an official agitation and propaganda commission within the Central Committee of the Communist Party. This newly established unit was called Agitrop, and its main mission was to direct and coordinate the main propaganda activities of Soviet-style institutions.

Later, after the dissolution of the Comintern in 1943, a new institution appeared called the International Department of the Central Committee of the CPSU, with the role of coordinating the methods and means of transmitting propaganda in states outside the USSR. Thus, the International Department was becoming a very important institution, with a much more precise and detailed role than that of the Ministry of Foreign Affairs of the USSR. It is known that until 1979, the institution called Agitprop had the mission of carrying out propaganda on the domestic territory, and the International Department both in friendly communist countries and in enemy countries. The dissemination of Soviet propaganda was achieved through agents of influence, such as the World Peace Council, the World Federation of Teachers' Unions, the

International Organization of Journalists, but also through networks of local organizations, from press clubs to various Soviet friendship societies (Shultz & Godson, 1984).

In addition to the influence manifested within this information, covert influencers were also used to spread disinformation and propagate false ideas. This orientation of the propaganda activity was ensured by the Political Bureau of the Communist Party and the State Security Committee (Voicu, 2018). During the Second World War, the USSR pursued, in addition to the neutralization of Nazi Germany and the achievement of revisionist objectives, using in this sense various Soviet Societies established with the aim of spreading propaganda and carrying out acts of intimidation. The so-called Soviet Societies were established since 1939 (Troncotă, 2004) in the United States of America in four large cities (New York, San Francisco, Chicago and Saint Louis). These centres aimed to carry out propaganda in favour of the USSR. Including the Society of Bessarabia established by the Soviets campaigned in favour of the right to self-determination of the Bessarabian people, and through various manifestos and memos they were preparing to influence American public opinion. Including, the Inter-Balkan Bureau of Minority Agitation functioned in Bucharest, whose aim was the intentional production of agitation, dissatisfaction among the workers who carried out their work for the state institutions. Thus, regarding the USSR we can distinguish the following actions (Troncotă, 2004):

- The USSR used the Pan-Slavic issue in political actions as a way of expansion in Eastern Europe and the Balkans;
- The Third International was involved in an active propaganda process by which it supported the world-wide revolution and wanted the imposition of the proletariat.

Russian propaganda, component of hybrid warfare

Currently we are witnessing an increasingly accentuated revisionism on the part of Russia, this new orientation is determined by the so-called Gherasimov doctrine which includes many features of the hybrid war that Moscow is waging both in Ukraine and in countries of interest. Valeri Gherasimov, the Chief of the General Staff of the Russian Armed Forces gave a speech in 2013 (Galeotti, 2016), clarifying the way of action and approach of the Russian Federation in the war of the contemporary era,

where there are no clear borders or well defined, and military operations do not copy a specific model.

Thus, Gerasimov's speech provides insight into the fact that "the rules of the game have changed" and the current security environment is defined by the changing nature of conflict. The vision focuses on the idea of using the protest potential of the population, together with akinetic means (Medar, 2018) to generate political, religious, social and economic tensions. Gherasimov talks about a technology of disruption, which involves a strong and specific component, intended to create a cooling of relations between the so-called adversaries of Moscow among the population, especially within Russian ethnic minorities (Galeotti, 2016). However, these particularities enunciated above are not necessarily new, many of them being enunciated by Colonel Evgheni Messner since the Cold War period. He was a theorist and thinker who understood the importance of popular movements, and in his view the most important battle is in the minds of the people, while the main fronts are behind enemy lines and contain a political, social and economic substance. Messner's theory of influencing the perceptions of the civilian population contrasts with the conventional way of understanding war, based on the conquest of territories. Thus, propaganda along with disinformation are used to create a society where propagandists have freedom of movement, being able to capitalize on the grievances of the population, amplify disapproval and discourage any actions against Russian power.

The anti-Bolshevik colonel Evgheni Messner (1891-1974), a former career soldier in the Tsar's army and theorist, developed a new theory about the notion of war in the middle of the last century: "In the wars until now, the conquest of territories was important. From here on, the most important thing will be winning the minds of those who are in the enemy state" (Messner, 2015, p. 40). This vision of Messner is one of the new methods that Russia is constantly applying in areas of interest, including Ukraine.

Theory of Reflexive Control

Disinformation, propaganda, information operations represent a strategy of action of the hybrid war pursued by the Russian Federation at the global level. Propaganda is one of the most important components of hybrid warfare, and the efficiency of this means is due to the fact that

the adversary cannot anticipate and counter the disseminated message in time. Thus, the propaganda messages developed by the Russian Federation through its various channels, but also through certain agents of influence, are very well anchored in the current political, social, technological, economic and religious particularities of the targeted state.

The theory of reflexive control (TCR) represents a way of influencing the decision-making act of the adversary, and this mechanism involves the transmission of information (fabricated data), which causes the enemy to resort to a variant favourable to the initiator of the action. The theory of reflexive control is an essential principle frequently used in most propaganda, manipulation and disinformation actions by the Russian Federation, even during the Cold War (Nicolescu, 2017, p. 25).

One key goal of a government is to actively engage in the decision-making processes of an opposing state. This objective is achieved by the Russian Federation through the use of information warfare based on the theory of reflexive control. The most complex form of influencing the informational resources of a state consists in the use of reflexive control measures against the decision-making factor. An information resource is best defined by (Thomas, 2004):

- all information and the means of transmitting information, which include methods of gathering, obtaining, processing, analysing, transmitting, capitalizing and storing;
- infrastructure consisting of centres and means of automating information processes, information switches and data transfer;
- computer programs and mathematical means for information management;
- the administrative and organizational body that manages the information process, the scientific staff, the databases, as well as the staff that serves the information means.

The theory of reflexive control represents a method with a major impact in approaching reality, and among the tactics used are: determining the enemy to approach a certain strategy, transferring an image onto reality, influencing in making a decision. Among these methods there are other ways such as: transmitting false information, carrying out information dissemination at certain key moments, projecting a non-conforming reality or an altered image that contradicts reality. The theory

is based on the principles stated by Pavlov Ivan Petrovici, author of the conditioning theory (Stamatin, 2017). Thus, TCR implies the exercise of control over an actor on the international stage by transmitting a certain informational stimulus.

The theory of reflexive control is a key element of the information warfare that the Russian Federation uses on a global scale. Through this technique, the Kremlin wants to take advantage of all the social, psychological, moral, religious vulnerabilities that it exploits to the maximum. The successful application of the technique consists in knowing the enemy from a social and psychological point of view, having a consistent volume of information about him, about his ability to analyse the events around him, but also the level of precise observation of certain stimuli that can provoke reactions.

The theory of reflexive control differs from other concepts of the informational war in that through the circulated information it is aimed to determine the modification of the decisions related to the decision-making factor. Thus, propaganda and disinformation aim to influence the population, while TCR focuses on influencing the decision-making factor.

Reflexive Control – instrument of the Russian Federation

In recent years, as a result of the Russian Federation's invasion of Ukraine, international interest in the Kremlin's hybrid warfare has increased. At first, this modus operandi of the Russians was treated as something new, but analysts noted the similarity of the current methods with disinformation and propaganda tactics used by the Soviets in the past (Minton, 2017). Thus, the Russian Federation uses the theory of reflexive control from the Soviet period, but connected to the realities existing today. The key element of TCR is the use of propaganda and disinformation. Disinformation can be divided into two categories: offensive and defensive. Offensive disinformation seeks to influence foreign public opinion and decision makers, while defensive disinformation is primarily aimed at influencing the Russian population (White, 2016). For example, Russia Today (RT) is a Russian government-funded news site whose purpose is to spread disinformation and

propaganda using the Kremlin's perspective on global events. Former Russian blogger Anton Nosik considered Russia Today to be a "Soviet-style propaganda agency dating back to the days of Joseph Stalin" (Minton, 2017, p. 5).

Soviet reflexive control contained specific strategies for both domestic and foreign policy. Domestically, influence consisted of the defensive use of propaganda and disinformation. This was possible by altering reality, altering the truth and creating a new reality. In the Soviet Union, the government propagated ideas and messages through newspapers, radio and restricted any access to Radio Free Europe. The same methods are still used today, but connected to the realities of the 21st century. Due to the fact that the world has evolved, and the main source of information has moved from the radio to the Internet, the Russian Federation blocks the Internet protocol addresses of some foreign sites. In addition to the information they follow on the Internet, the Russian population watches news bulletins on television. As a way to defend itself, the Russian government has banned all foreign nationals from owning any media companies in Russia (Minton, 2017).

The disinformation and offensive propaganda that Moscow is intensively promoting is the main concern of the international community. To achieve offensive propaganda through reflexive control, the Kremlin uses what Snegovaya (2015), call the 4D approach (dismiss, distort, distract, dismay). At the moment of the appearance of data and information related to the actions of the Russian Federation, members of the Government come out publicly and deny any accusation. An example is the accusations dismissed by the President of the Russian Federation, Vladimir Putin in the case of the occupation of Crimea by Russian militants (White, 2016). Thus, Russia constantly tries through propaganda, fake-news and disinformation to distort certain ideas, facts, data that are against their interests, with the aim of distracting the attention of both countries and international bodies. In addition to the classic 4D approach, two new forms seem to have emerged: destruction and destabilization (Snegovaya, 2015). Russia combines destruction and destabilization as part of its propaganda and disinformation technique to change the international system of the balance of power.

Background and objectives of Russian propaganda

The Russian Federation is engaged worldwide in a powerful propaganda campaign. The Kremlin's information warfare operations are an extremely important chapter of foreign policy, and online social media is where Russia exerts its control. Information warfare analyst Timothy Thomas stated that: "A veritable cognitive war is being waged in the airwaves and mass media for the hearts and minds of its citizens both at home and abroad" (Thomas, 2014, p. 12). Another analyst on the eastern space, the British Keir Giles was of the opinion that: "Russia considers itself to be engaged in a full information war" (Giles, 2016, p. 23).

In the information war in which it is involved, Russia uses various techniques such as: propaganda, cyber operations, disinformation, with the aim of influencing its neighbours and the countries of Western Europe. The state-funded television network Russia Today (RT) broadcasts global news in various languages (Arabic, English, Spanish). The Russian state also controls online news sites such as Sputnik, spreading its own news in over 30 languages. In addition to these elements, Russia uses cyber operations on a large scale, with Russian trolls playing a prominent role. The Russia Today and Sputnik networks were thought of as tools to broadcast information in various languages and through which the Kremlin can attack democratic values and spread false information (Christopher & Matthews, 2016).

The Russian state began to attach increasing importance to the media following the anti-government protests that took place in 2011 (Giles, 2016). The Internet was thus becoming an instrument of democratization and a way through which people censored by their own states could organize and protest. The scale and dynamics of the protests, amplified by the role of the mass media, led the Russian government to increase its actions and efforts to increasingly monitor, control and influence the virtual environment and social media. In the 2011 demonstrations, Russian citizens mostly organized on Facebook, took to the streets, and protested the elections that saw Vladimir Putin regain the presidency. Thus, in order to exercise this control effectively, the Kremlin has begun its offensive on the Internet and has invested in personnel, technology, and developing an army of trolls and bots, a kind of commentators paid to intervene with various opinions in comment

sections on social networks, but also on certain foreign news sites. The government has been involved since 2012 in a vast propaganda campaign in the virtual environment by establishing internal control, and externally influencing public opinion (Giles, 2016).

Although Russia seems to have a global aim in terms of propaganda campaigns, the area of major interest is the states in its immediate vicinity. The close neighbourhood refers to numerous Central Asian states such as: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Transcaucasia (Armenia, Azerbaijan and Georgia), Belarus, Republic of Moldova, Ukraine, Estonia, Lithuania, Latvia (Pomerantsev, 2014). These states express their concern especially that the Russian Federation has annexed the Crimean Peninsula and is actively involved in the Ukraine War through a hybrid war that combines kinetic elements (green men) with akinetic elements (propaganda, fake news, disinformation) (Medar, 2018).

Russia has various reasons for using the phenomenon of propaganda in former communist countries. These are:

- influencing the political class, the citizens of these states – helps to establish a buffer zone that ensures security against the influence of NATO and the EU, which is perceived a threat to Russia;
- in many of the former communist countries there is an important Russian-speaking minority population, and propaganda acts effectively on them.

The Kremlin pursues a policy of protecting the interests of the Russian minority population and thus tries to effectively influence the policy of neighbouring states.

Russian propaganda instruments

As far as Moscow is concerned, propaganda, fake news, disinformation and cyber-attacks are essential to achieving its own goals. The activities stated above are carried out with the help of trolls (social media accounts behind which certain people are) and bots (automated programs), which operate in the online environment on social networks, with the aim of exploiting vulnerabilities, transmitting certain information and strengthening credibility in messages subject to misinformation (Giles, 2016). The Russian Federation makes extensive use of fake social

media accounts that are fully or partially automated, or operated by handpicked individuals. This mechanism of Russian propaganda deserves a very careful examination in order to correctly and concretely understand how the propaganda machine works. Moscow's orientation towards the specific activity of information warfare results from the confirmation of the fact that "the virtual environment has become the main and only channel of information and political communication for a growing number of young people. In the virtual environment, they receive primary information, here they shape their visions and political opinions, having the opportunity to influence the processes related to the functioning of power." (Velichka, 2012, p. 55)

Thus, the life of a troll employed by Moscow requires making numerous comments, posts from different accounts to create an authentic and real appearance of the people who do this. The troll factory is based in St. Petersburg, and employees are paid at least 500 dollars per month to handle various fake accounts. In a 12-hour shift, a troll generates hundreds of comments, and sometimes they operate in mixed teams of three people on a particular topic. Thus, on a certain political or social topic, one of the trolls shows a negative point of view, while the other two trolls disapprove of it and thus creates the feeling of a debate (Aro, 2016).

A study carried out by NATO's Strategic Communication Centre aimed to observe and evaluate the impact of the activity of Russian trolls in cyberspace. In this study, approximately 3 671 articles and comments referring to the annexation of Crimea or the war in eastern Ukraine posted on a variety of Russian, Lithuanian, Polish, Estonian social networks were examined. The study found that these troll comments automatically generated a significant increase in comments from real people, who were practically invited into the discussion (Szwed, 2016).

It was also noticed that if Russian trolls used denial techniques, amplified hatred, denigrated the enemy's image on a post, it had many comments. In the first phase, a troll posted a certain negative message, which generated controversy and attracted the attention of other users, prompting them to comment based on the topic. The next step was to attract other users to counter the previous comments and thus create conflicting opinions. The last stage was based on deviating from the topic

of the respective article, thus, instead of creating a contradictory discussion, they generated strong antagonisms among users. In addition to the mode of operation of the trolls, the NATO study also identified the following behaviours of them (Szwed, 2016):

- transmission of certain information without reference to credible sources;
- posting certain links without other comments;
- sending off-topic messages;
- involvement in discussions about conspiracy theories;
- generating conflicts and intimidation through posts;
- claimed to be pro-Ukrainian, provoked others and generated responses from pro-Russian users.

Russian trolls have diversified and perfected their modus operandi to be more efficient, effective and to have a much greater impact. Thus, four types of trolls have been identified (Boffey, 2016):

- trolls who accuse the United States of conspiracy to create a feeling of mistrust;
- aggressive trolls who harass, induce negative ideas and participate in online discussions;
- Wikipedia trolls who edit sites, web pages to the advantage of the Kremlin;
- attachment trolls who linked their posts to Russian sites.

Russian propaganda is repetitive, fast, and continuous

The main characteristics of Russian propaganda are: repetition, rapidity and continuity. Thus, the repetitiveness of propagandistic message dissemination leads to familiarity, and familiarity leads to public acceptance. Russian propaganda is always based on creating a first impression, which is very durable and difficult to change.

Nowadays, the actions of the Russian propaganda machine are based on continuity, on the quick response of trolls, on the lack of coherence, but also on the lack of commitment to objective reality. Based on the characteristics stated above, Russian propagandists do not aim to verify the veracity of the facts, but pursue their presentation with great speed and precision so as to fully and correctly support their objectives.

Thus, the formidable ability to transmit "first news" is determined by the remarkable agility and responsiveness of Russian trolls.

The existence of numerous propaganda materials disseminated in the media space by Russian propagandists was observed (Paul & Matthews, 2014). These fake materials included a so-called statement by President Andrzej Duda demanding that Ukraine cede former Polish territory that belonged to it, as well as false information that Islamic State fighters had joined forces in Kiev (Paul & Matthews, 2014).

In some situations, the dissemination of Russian propaganda falls to certain news channels that take certain information, stories and broadcast them as if they are legitimate and true. Later, in the virtual environment, on social networks, trolls come into action and resume the themes covered by the news channels, amplifying the topic even more, giving it a negative connotation (Zorina, 2015).

From a psychological point of view, first impressions are the most important and determine a resistance over time. Thus, a person is very likely to accept the first information about a topic, give it credence, and expose or support it when faced with conflicting information (Petty, Cacioppo, & Strathman, 2019). However, repetition leads to familiarity which then turns into acceptance (Paul & Matthews, 2014):

- Repeated presentation of a state, reality or facts about a certain theme, considerably increases the level of public acceptance.
- The "illusory truth effect" refers to the fact that people consider some statements to be true, valid and credible when they have encountered them before and in the past than when they access them for the first time.
- When people are less interested in a topic, they tend to accept information with which they have become familiar over time (familiarity produced by repeating that information).
- When processing information, individuals can save time and energy by using a frequency heuristic, which refers to favouring information that they have heard repeatedly in the past.
- Even when exposed to "outlandish" stories and legends, people who have heard them repeatedly in the past are more likely to believe them to be true.

- When an individual is familiar with a certain idea or claims to be familiar with it (just because they have heard of it in the past), they tend to process information about that idea more superficially, often giving it more credibility weak arguments against strong ones.

Russian propaganda has the characteristic of being agile, fast and continuous, which allows propagandists to create a first impression. Subsequently, rapid responsiveness is correlated with a large volume of information, with a variety of dissemination channels. All these together make Russian themes very popular among the audience, thus giving them an extra boost in terms of credibility and expertise.

Objectives of the Russian Federation

The propaganda actions carried out by the Kremlin have the main purpose of supporting the foreign policy of the Russian Federation both in the mass media inside the country and abroad by transmitting relevant information aimed at Russian citizens outside the country. The Russian Federation maintains the tradition of the Soviet era and seeks to influence its adversaries through the extensive use of propaganda and disinformation. This tradition is also doubled by the statement of General Valeri Gherasimov, the Chief of Staff of the Army, who explained that the role of non-military means has increased, surpassing the power of weapons in many cases (Van Harpen, 2016).

One of the main goals of the Russian Federation is to have the status of a world power, and as part of this effort, it intends to restore its influence over the former territories dominated by the Soviet Union.

Russia also identifies NATO as a major threat to national security, being against certain international organizations. It believes that any nation must defend its own position in the international system. Thus, weakening the European Union and its member states is one of the main objectives of Russian propaganda. Moscow's strategy is to weaken the unity of the EU member states, because in a divided Europe, the Russian Federation could use a strategy of division, aiming to expand on the European continent. Russia's advantage is to have a military superiority over any other nation on the European continent (Cioroianu, 2009).

The Russian Federation aims to block any possible colour revolution that might take place in the former Soviet republics. They

represent the immediate vicinity that the Putin regime considers to be part of their sphere of influence. The concept of "Russkiy Mir" can also refer to the fact that national borders are of little importance for ethnic ties, thus the expression defines Russia not as a country, but as a community of people. This concept is again used by the Russian administration as a tool in its relations with former USSR countries (Courtois & Ackerman, 2017).

Identifying Russian propaganda

It is important to identify the official channels that belong to the Russian state, such as Russia Today and Sputnik, in order to be able to determine exactly which narratives are addressed in a certain period of time. These news agencies are professional because of the manner in which they present their messages, but they are not objective, they are biased like unofficial propaganda sites. Sputnik and RT amplify the voices and statements of certain pro-Russian MEPs, and in some broadcasts, they take only those quotes of European representatives that they take out of context. The views and comments of European politicians who have criticized the Kremlin are not included in the TV programs broadcast in the Russian state. The interviews broadcast on Russia Today or Sputnik mainly feature politicians who give statements in favour of Russia. Later, on social media networks these statements are picked up and falsified with the obvious purpose of misinforming (Cull et al, 2017).

Russian propaganda sites generally deal with a number of common topics: Ukraine, Syria, migration, the European Union and NATO, liberalism and liberal media. Alternative sites usually justify and legitimize the Kremlin's actions and views, and in other cases offer completely different narratives about the same events to create confusion. Propaganda sites also spread conspiracy theories that often attract public attention. Conspiracies are illegitimate, invented theories that are a temptation for all people, although many consider themselves resistant to such methods (Makukhin & Tsybulska, 2018).

For the manipulation of individuals, the Russian propaganda machine fakes pictures, videos, etc. Mostly, pictures or videos are modified with the help of software. In addition, sites upload images or

videos that depict events unrelated to the content of the article, which may even be taken in other locations or on different dates. It is possible to misinform readers through a wrong translation (for example, Arabic to English translation). It is very important that readers access original content as much as possible (Makukhin & Tsybulska, 2018).

In addition to the above, pro-Russian sites falsify or manipulate data, statistics, figures, surveys to justify their point of view. They regularly and continuously try to draw wrong and completely untrue conclusions from public opinion polls.

It is very important that before reading an article, news or document we try to accurately establish the credibility of the sources, to determine who the author is and whether he is real. Some sites link to anonymous blogs, pro-Kremlin propaganda sites, Facebook posts or extremist sites. In these cases, the sites admit that the source of inspiration was represented by the Western European media. Propaganda sites also claim that the information disseminated is taken from official sources, but in fact this is just a manipulation, since most of the time there is no connection with specialized institutions. Many times, countless people interviewed by the pro-Kremlin media appear in different poses and roles (intentionally changed), and it is quite possible that some of their words are taken out of context or translated differently. There are various allegations (Cull et al, 2017) directed at the pro-Kremlin media, being suspected of paying people to report certain events in an interview.

First Draft News, a fake news checking agency identified seven types of disinformation methods that pro-Kremlin media use. These are as follows (Barclay, 2018):

1. The first type of disinformation refers to false links, where titles, images, videos or translations are inconsistent with certain parts of the article.

2. The second method of disinformation refers to the false context, when a certain authentic informational content is correlated with an untrue or non-existent context or event.

3. The third method is manipulated content, and information, data, statistics or images are altered with the aim of deceiving readers and changing certain perceptions.

4. The fourth variant is represented by satire, parody, through which the aim is to influence individuals without causing any harm.

5. The fifth method involves the use of misleading content that formulates a problem through the information circulated.

6. The sixth method refers to falsifying truthful sources and replacing them with false and untrue ones.

7. The seventh method is to 100% modify a material and disseminate it to create uncertainty and harm.

Russian propaganda is complex because it often combines pieces of accurate information with false information. Thus, authentic information is manipulated by taking facts out of context and analysing them in a way that paints an incorrect picture of events. For the fake-news phenomenon to generate important changes and to be successful, it is necessary to establish a certain form of credibility. Many times, a particular news story is completely fabricated.

Methods and practices for combating Russian propaganda

Over time, both rational and ludicrous arguments have been observed to be effective in spreading conspiracy theories. Reality still matters, but it is difficult for some people to differentiate between true facts and alternative facts. Analysing the ultraconservative image of the Russian Federation, one can see the kleptocratic nature of Putin's regime, the declining birth rate, the social problems that bring Russia closer to the aging Western societies, from which it wants to distance itself (Kochis, 2014). Even though Russian propaganda does not necessarily seek to convince the public, it is very important to be able to identify the different narratives made to describe a particular event. The Russian government uses the lies spread to achieve its own goals.

First of all, to notice and discover a Russian propaganda material we need to focus our attention to the photos in the online environment that are most popular on social media. In order to establish the credibility of these photos, we must carefully analyse and try to get information from other sources in order to find other images related to that event (Bodine-Baron et al, 2018).

Second, other information should be sought in connection with the videos posted on pro-Kremlin sites, finding the original ones on YouTube or other networks is very important. In addition to these, it

is necessary to check the date the video was uploaded, its description, but also the license, to determine if the video was taken directly from the source (Bodine-Baron et al, 2018). Afterwards, you have to go to the comments section to see if someone has uploaded the original video.

Thirdly, attention should be paid to witness statements and interviews of certain people featured in reports on Russian propaganda sites and channels. It is imperative to determine whether the testimony or interview is closely related to the content of the article and whether there is any difference between the interviewee's statement and what the report claims. In addition to these, translations are a means of influence, therefore transposition verification should not be ignored (Bodine-Baron et al, 2018). Another way to identify the influence of Russian propaganda is to identify the roles played by some witnesses. There are numerous people paid to support the Kremlin's point of view.

Regarding the method of citing individuals, it is important to check whether the quote has been taken out of context. Thus, the material must be viewed and read carefully. The experts and sources used by the pro-Russian sites must be investigated. The experts that the pro-Russian sites cite mostly serve the interests of Moscow, and in other cases the source of the citation is a prestigious European magazine, but in reality, the citation refers to a lesser-known blog with a similar name (Kochis, 2014).

In conclusion, Russian propaganda employs various tactics, including information pressure (repeated dissemination of news), information intoxication (overloading with true and false data), rumour transmission (rapid circulation of rumours), erosion of trust in leaders (revealing half-truths or lies about trusted figures), and an appeal to history (presenting false information about Romanian Army actions in World War II).

In contrast to Soviet-era propaganda, contemporary propaganda exhibits a heightened level of conviction, superior organization, and strategic planning, employing a diverse array of manipulation and influence techniques. Unlike the past focus on disseminating processed information to gain support for the communist regime, modern propaganda is prominently present in the virtual sphere, with its primary objective being to induce a state of confusion rather than convince the target audience.

References:

1. Barclay, D. (2018). *Fake News, Propaganda, and Plain Old Lies: How to Find Trustworthy Information in the Digital Age*, Rowman & Littlefield, London.

2. Bodine-Baron, E., Todd, C., Radin, A. & Treyger, E. (2018). *Countering Russian Social Media Influence*, RAND Corporation, Santa Monica, Calif.

3. Boeffy, D. (2016), *Europe's New Cold War Turns Digital as Vladimir Putin Expands Media Offensive*, Guardian, retrieved from: https://www.theguardian.com/world/2016/mar/05/europe-vladimir-putin-russia-social-media-trolls.

4. Cioroianu, A. (2009). *Geopolitica Matrioșkăi: Rusia postsovietică în noua ordine mondială*, Curtea Veche Publishing, Bucharest.

5. Courtois, S. & Ackerman, G. (2017). *Discursul politic rus de la al Doilea Război Mondial la conflictul ruso-ucrainean*, Polirom Publishing, Iași.

6. Cull, J., Gatov, V., Pomerantsev. P., Applebaum, A. & Shawcross. A, (2017) *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It*. The London School of Economics and Political Science, retrieved from http://www.lse.ac.uk/iga/assets/documents/arena/2018/Soviet-Subversion-and-Propaganda-how-the-west-thought-against-it.pdf.

7. Galeotti, M. (2016). "Hybrid, ambiguous, and non-linear? How new is Russia's new way of war?", *Small Wars & Insurgencies*.

8. Giles, K. (2016). *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, Russia and Eurasia Programme, March, retrieved from https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

9. Kochis, D. (2014). *Countering Russian Propaganda Abroad, The Heritage Foundation Massachusetts Avenue*, NE Washington, DC 20002, retrieved from https://www.heritage.org/europe/report/countering-russian-propaganda-abroad.

10. Makukhin, O. & Tsybulska, L. (2018). *How Russian Media Foments Hostility Toward the West Hybrid Warfare Analytical Group*, The Black Sea Trust for Regional Cooperation, retrieved from http://ucmc.org.ua/wp-content/uploads/2018/02/TV-II-n.pdf.

11. Medar, S. (2018), *Noua ordine internațională a lumii, Monitorul Apărării şi Securităţii,* retrieved from https://en.monitorulapararii.ro/world-s-new-international-order-1-5224.

12. Messner, E.E. (2015). *Razboiul Răzvrătirii mondiale*, Antet Revolution Publishing, 2015.

13. Minton, N. (2017). *Cognitive Biases and Reflexive Control,* retrieved from http://thesis.honors.olemiss.edu/869/1/SMBCH%20Final%20Thesis.pdf.

14. Nicolescu, F. M. (2017). "Războiul hibrid. Perspectiva conceptuală rusă", *Intelligence Journal*, retrieved from https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa/

15. Paul. C. & Matthews, M. (2014). *The Russian Firehouse of falsehood Propaganda model*, retrieved from chrome-extension:// efaidnbmnnnibpcajpcglclefindmkaj/https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

16. Petty, R., Cacioppo, J., & Strathman, A. (2019). *To Think or Not to Think Exploring Two Routes to Persuasion*, retrieved from https://www.researchgate.net/publication/237406179_TO_THINK_OR_NOT_TO_THINK_Exploring_Two_Routes_to_Persuasion/download.

17. Pomarantsev, P., Weiss, M., (2014)."The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money", *The Interpreter*, retrieved fromhttp://www.interpretermag.com/wpcontent/uploads/2014/11/The_Menace_of_Unreality_Final.pdf

18. Sazonov, V., Müür, K. & Mölder, H., (2015). *Russian Information Campaign Against the Ukrainian State and Defence Forces*, NATO Strategic Communications Centre of Excelence, retrieved from https://www.stratcomcoe.org/russian-information-campaign-against-ukrainian-state-and-defence-forces.

19. Snegovaya, M. (2015). *Putin's Information Warfare in Ukraine*, Institute for the Study of War, retrieved from: http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdfThomas.

20. Shultz, R. & Godson, R. (1984). *Dezinformatsia. Active measures in Soviet Strategy*. New York: Pergamon Brassey's Publishing.

21. Szwed, R., (2016), *Framing of the Ukraine–Russia Conflict in Online and Social Media*, Riga, Latvia: North Atlantic Treaty Organization Strategic Communications Centre of Excellence, retrieved from http://www.stratcomcoe.org/framing-ukraine-russia-conflict-online-and-social-median.

22. Thomas, T. (2014). "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations", *Defence Strategic Communications*, Vol. 1, No. 1, Winter 2015, pp. 11–26. As of November 7, 2017, retrieved from https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations.

23. Troncotă, C. (2004). *Mihail Moruzov şi frontul secret*, Bucharest, Elion Publishing.

24. Van Van Harpen, M. (2016). *Putin's Propaganda Machine; Soft Power and Russian Foreign Policy*, Rowman & Littlefield, London.

25. Velichka, M. (2012), *Security in a Communications Society: Opportunities and Challenges'*, Connections, Vol. 11, No. 2, Spring 2012.

26. Voicu, M. (2018). *Matrioşka Mincinoşilor: Fake news, Manipulare, Populism*, Bucureşti: Humanitas Publishing.

27. White, J. (2016). "Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation", *Institute for European Studies*, Issue 2016/13, retrieved from https://www.ies.be/files/Policy%20Brief_Jon %20White.pdf.

PRACTITIONERS' BROAD VIEW

FIŞE INTEROGATIV-EVALUATIVE ALE FACTORILOR RELEVANŢI PENTRU STRUCTURILE INFORMATIVE/DE LAW ENFORCEMENT

Florin BUŞTIUC*
Alexandra POPESCU (ANGHEL)*

Abstract:
In their specific activities, the informative/law enforcement structures relate to the scenario of an operative reality on which they appear and evolve, on certain spatio-temporal coordinates: persons, groups, activities, goods and services, and events.

In order to effectively identify and assess threats, risks and vulnerabilities, a simple tool is needed to interrogate the operational reality, to generate appropriate responses that allow decisions and optimal knowledge, prevention and combat/ countermeasures. The tool consits of analytical evaluative sheets, with sets of interrogative items that inventory the complexity of reality, so that experience and knowledge are systematically capitalized, avoiding, as far as possible, the adoption of the decisions and measures in the absence of sufficient knowledge.

Keywords: *threats, operative reality, adversaries, places and interest media.*

Introducere

Serviciile de informaţii (respectiv, structurile informative departamentale) desfăşoară activităţi de culegere/colectare/obţinere de informaţii, potrivit competenţelor legale, pentru identificarea disfuncţiilor, vulnerabilităţilor şi factorilor de risc ce se constituie în ameninţări, respectiv pentru cunoaşterea direcţiilor posibile de apariţie şi manifestare a respectivelor ameninţări pe dimensiunile de ordine publică, apărare şi securitate naţională (forme şi stadii, obiective, valori şi ţinte vizate, tipul

* PhD, "Mihai Viteazul" National Intelligence Academy, email: florinnn11@yahoo.com.
* PhD student, University of Bucharest, Doctoral School of Sociology, email: alexandra.popescu@drd.unibuc.ro.

de acţiuni şi modalităţi de realizare, consecinţe şi impact). Prin planificarea şi căutarea informaţiilor se stabilesc vectori posibili ai ameninţărilor, zone, locuri, medii de interes informativ şi surse relevante sub aspectul colectării de date operative, iar culegerea de informaţii componenta fundamentală a ciclului de intelligence (core-business-ul serviciilor de informaţii). Procesul de culegere de informaţii se realizează prin supraveghere tehnică şi fizică, lucrul cu surse secrete umane, modalităţi de explorare operativ-informativă, verificări în baze de date, consultări ale surselor deschise şi oficiale, relaţii parteneriale, rezultând aspecte despre persoane (fizice, juridice), grupări, medii, organizaţii, situaţii, evenimente, contexte etc. (Coldea şi Niţă, 2022, p. 81)[1]. În esenţă, prin culegerea de informaţii se configurează situaţia operativă, care se traduce prin filtrarea unei situaţii/realităţi[2] prin intermediul vulnerabilităţilor, ameninţărilor, riscurilor.

Astfel, din perspectiva *securităţii* – văzută ca absenţa ameninţărilor şi riscurilor la adresa existenţei, valorilor şi intereselor statului/ indivizilor (Sarcinschi, 2005) –, **situaţia operativă** reprezintă ansamblul *stărilor de fapt, acţiunilor/inacţiunilor şi circumstanţelor* conexe *entităţilor, zonelor, locurilor, mediilor de interes* dintr-un *domeniu de competenţă* (de la protejarea şi promovarea principiilor constituţionale, a stabilităţii sociale, economice şi politice, menţinerea ordinii de drept la siguranţa persoanelor, protecţia avutului public şi privat etc.)[3] care se raportează

---

[1] *Doctrina naţională a informaţiilor pentru securitate*, adoptată prin Hotărârea Consiliului Suprem de Apărare a Ţării din 23 iunie 2004 (cu Nota de fundamentare semnată de reprezentanţii Serviciului Român de Informaţii, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Pază, Serviciului de Telecomunicaţii Speciale, Ministerului Administraţiei şi Internelor Ministerului Apărării Naţionale, Ministerului Justiţiei).

[2] Definiţii disponibile la https://dexonline.ro: **realitate –** fapt, lucru real care există efectiv, stare de fapt; **situaţie** – totalitatea împrejurărilor (circumstanţelor) care determină la un moment dat condiţiile existenţei unei persoane, colectivităţi, activităţi; **stare** – situaţie în care se află ceva sau cineva la un moment dat; **stare de fapt** – situaţie dată, reală (fapt – lucru petrecut în realitate; împrejurare, întâmplare reală; circumstanţă concretă).

[3] *Strategia naţională de ordine şi siguranţă publică 2023-2027,* România, disponibilă la https://webapp.mai.gov.ro/frontend/ documente_transparenta/547_1679910354_Proiect %20SNSOP%202023-2027%20%20martie%202023.pdf; *Strategia naţională de ordine şi securitate publică 2017-2020,* Republica Moldova disponibilă la https://gov.md/sites/ default/ files/ document/attachments/intr20_71.pdf.

la *cunoaşterea, prevenirea şi contracararea/combaterea ameninţărilor, riscurilor, vulnerabilităţilor (Glosar de termeni din domeniul ordinii şi siguranţei publice*, 2006, p. 248; Cristescu, 2000, p. 83). Nivelul, caracteristicile şi tendinţele de evoluţie ale situaţiei operative se pot exprima pe dimensiuni de tip geografic, pe structuri funcţionale, procese şi activităţi, în mod descriptiv sau prin indicatori specifici.

Din perspectiva detaliată a elementelor care compun situaţia operativă, avem: *factorii constitutivi* (persoanele, reţelele, grupările – entităţile, activităţile, bunurile şi serviciile, piaţa, fenomenele/ evenimentele), *coordonatele pre-stabilite* (spaţiale şi temporale), *factorii de activare a entităţilor* (mijloace de deplasare, mijloace de comunicare, resurse relaţionale, resurse financiar-materiale, acces), *factorii de structurare* (pattern-urile, trend-urile, schimbările, asocierile şi fluxurile), *factorii operativi* (ameninţările, vulnerabilităţile, riscurile).

Structurile informative/de law enforcement au ca scop cunoaşterea, controlul şi evaluarea situaţiei operative pentru a formula concluzii/ decizii şi a-şi stabili obiective, sarcini şi măsuri concrete în ceea ce priveşte contracararea activităţilor unor entităţi adverse (de la servicii de informaţii străine la grupări de criminalitate organizată) (Vezi detalii la Stambert, Dragu, Găitan, 2010, p. 228).

Factorii constitutivi ai situaţiei operative

Factorii constitutivi ai situaţiei operative sunt următorii: persoanele, reţelele/grupările, activităţile, bunurile şi serviciile, piaţa, fenomenele/evenimentele.

1. Analiza persoanei (Bărbuţă şi Marin, 2014, p. 117 şi pp. 203-204) se reflectă în identificarea unui individ ca prezentând elemente de risc (*vector*[4]*)*, urmată de iniţierea şi susţinerea unei investigări specifice până în momentul în care ameninţarea este eliminată (analiza se actualizează periodic/când este necesar pe baza datelor noi).

[4] Definiţii **vector de ameninţare / vector generator de ameninţare** – termen utilizat în Ordinul Directorului General al ORNISS nr. 16/2014 pentru aprobarea Directivei principale privind domeniul INFOSEC - INFOSEC 2, disponibil la https://orniss.ro/ro/ legislatie/pdf/ordine/ord_INFOSEC2.pdf. Vezi şi articolul *Perspective teoretice asupra ameninţărilor cu incidenţă în domeniul securităţii*, disponibil la https://intelligence.sri.ro/ perspective-teoretice-asupra-amenintarilor-cu-incidenta-domeniul-securitatii/

Pe baza analizei: se prioritizează selectarea vectorilor (principali şi secundari, legături); se identifică lacunele informative şi se direcţionează/ focalizează efortul de colectare a datelor; se orientează demersurile investigative şi deciziile de alocare a resurselor; se evidenţiază oportunităţile; se dezvoltă argumentele pentru diverse măsuri; se dezvoltă deducţii/ predicţii privind activităţile ilegale; se identifică potenţiale surse de informare; se asigură respectarea cerinţelor legale.

Fişă analitică tip interogativ-evaluativă – persoană:

- ☐ cine este individul şi care este statutul socio-profesional;
- ☐ dacă individul este membru al unui grup infracţional, care este mărimea grupului şi dacă există o structură ierarhică delimitată;
- ☐ dacă individul are o specializare anume sau abilităţi care îl fac important pentru funcţionarea unei activităţi sau reţele;
- ☐ dacă individul are un istoric infracţional;
- ☐ care sunt legăturile individului cu alte entităţi;
- ☐ ce caracteristici prezintă modul de operare (tehnici şi particularităţi comportamentale);
- ☐ dacă individul este implicat în activităţi pe o piaţă infracţională profilată şi caracteristicile acesteia (natura, mărimea, bunuri tranzacţionate, cantitate, calitate, preţ, metode de aprovizionare, de stocare, de comercializare etc);
- ☐ cum se realizează comunicarea, accesul la resurse, transportul şi distribuţia;
- ☐ care sunt locaţiile utilizate de individ şi rutele între acestea (domiciliu, reşedinţă, loc de muncă etc);
- ☐ care sunt sursele legitime de venit şi ce metode sau mijloace de plată sunt utilizate la efectuarea tranzacţiilor (dacă sunt indicii ale existenţei unor venituri ascunse);
- ☐ care sunt bunurile şi serviciile generate de activităţile ilegale infracţionale;
- ☐ dacă pot fi dezvoltate predicţii asupra comportamentului ilegal;
- ☐ dacă sunt fapte care au crescut ca frecvenţă ori ca intensitate;
- ☐ factori geografici, temporali, economici sau de mediu ce caracterizează/influenţează activitatea individului.

Obiectivul analizei persoanei este de a stabili, explica și interpreta: nivelul și gravitatea unei amenințări reprezentate de una sau mai multe persoane; o imagine de ansamblu asupra persoanelor analizate, inclusiv legăturile cu alte entități, mijloace de transport și de comunicare, bunurile și resursele financiare deținute, precum și istoricul activităților ilegale.

2. Rețeaua/grupul reflectă contactele/legăturile stabilite și menținute între diferite persoane, grupuri, organizații[5]. Analiza rețelei reprezintă identificarea, înțelegerea naturii și semnificației legăturilor între persoanele ce formează o rețea, sau între acestea și alte entități. Astfel, se construiește o imagine detaliată structurii, a caracteristicilor acesteia, a relațiilor dintre membri (de natură infracțională, de rudenie, de prietenie, de interese, financiară etc) și a rolului fiecărui membru (Bărbuță și Marin, 2014, p. 79 și 137, și 2014a, p. 104 -105).

Prin analiza legăturilor rețelei se realizează o descriere care vizează: „atributele și funcțiile cheie ale indiviziilor din cadrul rețelei; asociații din/în afara rețelei; punctele forte și vulnerabilitățile rețelei; analiza financiară și a datelor de comunicații; inferențe despre comportamentul infracțional în asociere cu profilul țintei" (UNDO, 2010, p. 21).

Un grup/o rețea este definit de următoarele elemente caracteristice (UNDO, 2010, p. 21):

- dimensiunea grupului (determinat în unele cazuri de zonă);
- structura/ierarhia grupului, determinată de compunerea, tipul și poziționarea membrilor;
- derularea unor afaceri legale și ilegale;
- valorificarea unor specialiști;
- exercitarea unor acțiuni de influență și corupție, structuri/ categorii de persoane vizate;
- existența și nivelul cooperării cu alte grupuri (și transfrontalier);
- utilizarea contramăsurilor, asigurarea protecției membrilor grupului și activităților.

Sintetic, analiza legăturilor rețelei: a) *la nivel strategic,* semnalează managementului gravitatea fenomenelor/actelor infracționale pentru formularea unor decizii strategice, b) *la nivel tactic și operațional*, infuzează

[5] Vezi definiții pe https://dexonline.ro/definitie/leg%C4%83tur%C4%83/definitii.

informaţii în operaţiunile care vizează ţinte, sugerează direcţii eficiente de investigare şi oportunităţi de destructurare, evidenţiază lacune în cunoaştere pentru a orienta valorificarea surselor/resurselor, dezvăluie modul de operare (cum sunt selectate ţintele, care este expertiza unor vectori, care sunt vulnerabilităţile exploatabile în sisteme sau proceduri). (UNDO, 2010, p. 21)

Fişă analitică tip interogativ-evaluativă – reţea/grup (Bărbuţă şi Marin, 2014, p. 79 şi 137):

- ☐ ce persoane compun reţeaua;
- ☐ care sunt persoanele implicate direct în activitatea infracţională şi jucătorii cheie;
- ☐ cum este structurată reţeaua;
- ☐ care sunt preocupările/scopurile declarate şi ascunse ale grupului şi în ce tipuri de activităţi ilegale esate implicat;
- ☐ cum se derulează activităţile reţelei;
- ☐ identificarea şi studierea legăturilor dintre entităţile reţelei
  - ✓ *legături de natură socială* – ce locuri frecventează, ce autovehicule folosesc, ce specialişti au cooptat în carul reţelei (pentru rezolvarea unor aspecte de natură financiară, tehnică, legală, autoprotecţie), care sunt modalităţile de comunicare (directă, curieri, telefonie fixă, telefonic mobilă, Internet), dacă folosesc limbaj codificat, dacă au posibilităţi de identificare a supravegherii, dacă au contacte în structurile de ordine publică şi securitate, dacă exercită acţiuni de corupţie sau influenţă la nivel local, regional, naţional sau internaţional.
  - ✓ *legături de rudenie* – cine sunt membrii de familie, ce ocupaţii au, unde locuiesc, dacă sunt implicaţi în activităţi infracţionale şi cât de strânse sunt relaţiile cu „jucătorii cheie".
  - ✓ *legături de natură infracţională* – dacă există o structură ierarhică în interiorul grupului, care sunt rolurile îndeplinite în reţea, activităţile grupului, ce cunoştinţe au persoanele din reţea despre metodele şi mijloacele utilizate de structurile informative/de law enforcement, cum cooptează grupul noi membri, ce mijloace sunt utilizate pentru a controla reţeaua.
  - ✓ *legături de natură financiară* – sursele de venituri legitime/ ilegitime, afacerile deţinute, metode de plată şi finanţare

(intern sau extern, volumul tranzacţionat), dacă există contabil al reţelei, dacă sunt indicii de implicare a reţelei în spălarea de bani sau în finanţarea unor alte activităţi (cine anume, cum se procedează), ce categorii de bunuri deţine reţeaua (licite sau ilicite), unde sunt conturile.

- ce posibilităţi are grupul/reţeaua să atragă noi membri;
- zona geogratică unde are sediul reţeaua, respectiv cea unde acţionează;
- ce locaţii sunt/au fost frecventate (locuri de întâlnire) şi ce mijloace de transport/rute sunt utilizate;
- când s-au petrecut evenimente importante din istoria reţelei şi ce natură au avut acestea;
- care este nivelul de utilizare a corupţiei şi care sunt legăturile cu activităţi similare legale;
- punctele tari şi punctele slabe ale reţelei;
- care sunt vulnerabilităţile reţelei (rivalităţi, dispute financiare, dispute de familie, de autoritate).

Analiza reţelei are următoarele obiective: să contureze o imagine detaliată a rolurilor deţinute de persoanele din reţea (ierarhia, poziţia în ierarhie şi nivelul de control deţinut); să indice asocierile între persoane şi entităţi din interiorul şi exteriorul reţelei; să indice vulnerabilităţile reţelei; să identifice persoanele care, dacă ar face obiectul unor măsuri, va determina periclitarea activităţilor/destructurarea grupului; să delimiteze zonele de acţiune a grupării, respectiv în care exercită influenţă şi control; să furnizeze o înţelegere a gravităţii ameninţărilor reprezentate de grupare; să sprijine procesul de selecţie al ţintelor; să direcţioneze colectarea de date, inclusiv evidenţierea unor potenţiale surse de informaţii; să furnizeze datele necesare fundamentării unor direcţii de acţiune şi măsuri adecvate pentru investigarea şi destructurarea reţelei.

3. Activităţile reprezintă un ansamblu de acte fizice şi intelectuale voluntare (sistematice) pentru a se obţine un anumit rezultat[6]. Analiza activităţilor furnizează o imagine de ansamblu asupra unui set de acţiuni sau moduri de operare, determinându-se care sunt elementele cheie care

[6] Vezi definiţii pe https://dexonline.ro/definitie/activitate/definitii.

concură la materializarea amenințărilor/activităților ilegale (Bărbuță și Marin, 2014a, p. 81; UNDO, 2010, p. 41).

Fișă analitică tip interogativ-evaluativă – activități (Bărbuță și Marin, 2014, p. 108):

- ☐ care sunt activitățile ilegale;
- ☐ când au început activitățile ilegale;
- ☐ care este scopul și motivația pentru desfășurarea activităților ilegale;
- ☐ în ce categorie poate fi încadrată activitatea ilegală și care sunt tiparele sau caracteristici comune care motivează încadrarea;
- ☐ dacă activitățile pot fi împărțite în diverse secvențe/etape și care sunt caracteristicile spațio-temporale ale acestora;
- ☐ există pattern-uri care inter-corelează caracteristicile spațio-temporale;
- ☐ ce schimbare în/a mediului a creat și/sau a crescut oportunitatea pentru apariția/dezvoltarea anumit tip de activitate ilegală;
- ☐ Care este organizația din spatele pattern-urilor? Cine sunt persoanele din spatele organizației? (organizațiile nu comit ilegalități, persoanele comit ilegalități).
- ☐ cine sunt organizatorii activității și de unde desfășoară activitățile;
- ☐ care este ierarhia indivizilor în organizație; care sunt jucătorii principali/cheie și care sunt cei mai puțin importanți;
- ☐ care este structura rețelei/grupului;
- ☐ care sunt persoanele ce au roluri specializate;
- ☐ cine a mai desfășurat anterior activități similare și care a fost scopul și motivația lor;
- ☐ cum sunt recrutați membrii rețelei implicate în derularea activităților;
- ☐ care sunt țintele - persoane etc;
- ☐ care sunt parametrii de desfășurare activităților – complexitate rețea, specializare membri, frecvență, profituri;
- ☐ dacă există conexiuni sau legături cu alte grupuri sau activități;
- ☐ unde sunt amplasate locațiile frecventate de membrii rețelei, locurile de întâlnire, proprietățile deținute, spațiile de depozitare;
- ☐ care sunt modalitățile de finanțare/plată pe plan intern și extern;

- care sunt metodele şi rutele de transport (inclusiv punctele de tranzit);
- care sunt metodele de comunicare şi elementele specifice de limbaj (cuvinte cu anumite semnificaţii);
- dacă ilegalitatea este orientată spre bunuri, unde sunt bunurile care sunt introduse în diferite circuite;
- unde, cum şi cine distribuie bunurile rezultate din activităţi;
- care sunt tiparele sau rutinele modului de operare;
- dacă sunt indicii referitoare la suportul din partea unor funcţionari din instituţiile de stat;
- dacă sunt indicii cu privire la cunoaşterea mijloacelor utilizate de către structurile de tip law-enforcement/informative;
- dacă activităţile au un trend ascended sau descendent;
- dacă metodele de desfăşurare a activităţii se modifică în timp şi cum anume se concretizează;
- ce alte date există şi cum afectează ipotezele de lucru (de exemplu, implicări anterioare în activităţi infracţionale, venituri ascunse etc).

Obiectivul analizei activităţilor este de a stabili, explica şi interpreta: rolul, tipul, complexitatea şi importanţa fiecărei activităţi; dacă sunt similitudini cu alte activităţi ilegale sau moduri de operare şi dacă există eventuale conexiuni cu acestea; stabilirea punctelor comune şi diferenţelor dintre elementele componente, în scopul identificării elementelor cheie; elementele relevante în desfăşurarea activităţilor, astfel încât prin intervenţia asupra acestora s-ar stopa/diminua activităţile.

4. Bunurile se referă la produse consumabile tangibile, articole, mărfuri (au caracteristici materiale), iar **serviciile** sunt facilităţi, beneficii furnizate de o persoană la cererea celeilalte persoane[7]. Analiza bunurilor şi serviciilor constă în evaluarea şi interpretarea caracteristicilor şi calităţii acestora (valoarea, disponibilitatea, proveniența, etc), pentru a înţelege valoarea materială sau psihologică pentru un subiect, raportat la nevoile şi aşteptările acestuia.

[7] Vezi detalii şi definiţii pe https://ro.economy-pedia.com/11031726-goods-and-services şi https://invatatiafaceri.ro/diferente/diferenta-dintre-bunuri-si-servicii/.

Fișă analitică tip interogativ-evaluativă – bunuri și servicii (Bărbuță și Marin, 2014a, p. 81):

- ☐ care este tipul și caracteristicile bunurilor sau serviciilor;
- ☐ principalele persoane implicate;
- ☐ care sunt sursele și canalele de aprovizionare;
- ☐ persoanele ce fac legătura cu alte organizații;
- ☐ locuri de plecare, tranzit, destinație și beneficiari finali;
- ☐ cum lucrează organizația sau persoanele implicate pentru a derula fluxurile de bunuri și servicii;
- ☐ rolurile entităților implicate în derularea fluxurilor;
- ☐ soliditatea legăturilor dintre entități prin prisma importanței și dinamicii fluxurilor;
- ☐ principalul beneficiar (din punct de vedere cantitativ&calitativ);
- ☐ care sunt prețurile (reale) și profiturile;
- ☐ care sunt reglementările referitoare la anumite bunuri și servicii, corelat cu prevenirea unor activități ilegale.

Scopul analizei bunurilor și serviciilor se reflectă în înțelegerea dimensiunii material-financiare a activităților desfășurate de subiecți/ entități, a conexiunilor cu alte entități în procurarea/ furnizarea de bunuri și servicii și a capacității de influențare în funcție de necesitățile existente[8].

5. Piața reprezintă totalitatea relațiilor generate de acte de vânzare-cumpărare sau tranzacționare, în conexiune cu spațiul în care se desfășoară[9]. Analiza pieței (market profile) punctează caracteristicile demografice și geografice ale unei anumite piețe sau industrii ilegale (de exemplu, traficul de droguri) și include date despre tipurile de *bunuri sau servicii, clienți/ consumatori, sisteme de prețuri și distribuție, competiție*.

Printr-o analiză a pieței se identifică bunuri/ servicii, surse de aprovizionare, jucători cheie, rețele, lanțuri de aprovizionare, pattern-uri ale unor rute, cu obiectivul de a se dezvolta evaluări și strategii eficiente de prevenire sau urmărire penală.

[8] Vezi detalii pe http://ec.utgjiu.ro/wp-content/uploads/2023/02/Microeconomie.pdf.
[9] Vezi definiții pe https://dexonline.ro/definitie/pia%C8%9B%C4%83/definitii.

Fişă analitică tip interogativ-evaluativă – analiza pieţei (Bărbuţă şi Marin, 2014, p. 107):

- ☐ cine sunt persoanele cheie implicate, care este ierarhia reţelei şi potenţialele vulnerabilitaţi ale acesteia;
- ☐ cum sunt implicate persoanele în activităţile de interes;
- ☐ unde anume opereaza persoanele cheie în piaţă (atât cu rol de furnizori cât şi de clienţi);
- ☐ care sunt ţintele;
- ☐ care sunt grupările/organizaţiile relevante şi care sunt legăturile stabilite în cadrul/între reţele;
- ☐ care este dimensiunea pieţei (nivelul infracţionalităţii, tipul, cantitatea, calitatea şi valoarea bunurilor oferite, frecvenţa de aprovizionare, furnizori, transportatori, trendul cererii şi ofertei, care sunt efectele de natură fizică, psihologică sau adverse ale bunurilor tranzacţionate);
- ☐ care este tipul pieţei (produsele şi serviciile oferite, dacă sunt prezente trenduri temporare sau ciclice, care a fost impactul acţiunilor anterioare ale structurilor de tip law enforcement/ informative):
- ☐ dispunerea geografică a pieţei (zone de tranzacţionare, locaţii frecventate, trasee de aprovizionare, moduri de operare folosite de furnizori şi transportatori, legături cu alte pieţe);
- ☐ care sunt produsele şi serviciile (tip, calitate şi cantitate, legături între anumite categorii de fapte şi bunurile tranzacţionate, ce metode şi mijloace de plată a bunurilor şi serviciilor sunt folosite etc);
- ☐ când şi unde au loc tranzacţiile din piaţă;
- ☐ unde sunt depozitate bunurile şi cum sunt furnizate;
- ☐ dacă sunt folosite metode de evitare a supravegherii sau a detectării activităţilor ilegale;
- ☐ ce trenduri şi pattem-uri au fost identificate în structura şi activitatea pieţei;
- ☐ dacă piaţa este organizată pe niveluri ierarhice şi cum este protejată ea de către persoanele/reţelele implicate.

Analiza pieţei are următoarele direcţii: a) agregarea unor profiluri standard a unor pieţe locale poate facilita construirea unei perspective de nivel superior şi b) poate genera o analiză mai detaliată în ceea ce

privește analiza profilurilor țintă, a tiparelor criminalității și rețelelor (UNDO, 2010, p. 21).

6. Fenomenul (evenimentul[10]) reprezintă manifestarea exterioară a esenței unui lucru, unui proces etc., care surprinde prin calități, noutate etc.[11] Analiza unor fenomene evidențiază și interpretează fenomene limitate si definibile, fiind orientată către identificarea cauzelor vizibile disimulate și modalităților de manifestare, organizare și evoluție (Bărbuță și Marin, 2014, p. 125).

Fișă analitică tip interogativ-evaluativă – fenomen (eveniment):

- ☐ s-a realizat încadrarea și evalurea istorică a fenomenului;
- ☐ s-a efectuat o evaluare comparativă cu fenomene similare;
- ☐ s-au identificat cauzele determinante ale fenomenului;
- ☐ s-au stabilit și examinat factorii de influență de natură socială, economică, geografică și administrativă;
- ☐ s-au identificat factorii care au facilitat apariția și/sau extinderea fenomenului;
- ☐ s-au constatat și examinat trenduri;
- ☐ s-au identificat măsuri eficiente pentru contracararea efectelor negative.

Obiectivul analizei fenomenelor este de a stabili, explica și interpreta: cauzele publice/ascunse, mecanismele de creare și amplificare, factorii de influență externi (economici, sociali, politici, tehnologici, ecologici etc) și interni (persoane, grupuri, organizații, relațiile existente, spațiul și momentul de manifestare etc), nivelul și tipul de control direct/indirect asupra factorilor, diagnosticarea în scopul fundamentării măsuri de influențare, diminuare și reglare (Robu, Georgescu, 2001, pp. 6-8).

Coordonatele pre-stabilite ale situației operative

Coordonatele pre-stabilite ale situației operative sunt următoarele: coordonate spațiale – *zone/locuri* și coordonate temporale – *trecut-prezent-viitor (momente-perioade)*.

---

[10] Apreciem că analiza de fenomen poate fi echivalată cu analiza unor evenimente (care reprezintă stări, fenomene importante / de mare însemnătate, de regulă instantanee sau neprevăzute - https://dexonline.ro/definitie/eveniment/definitii).

[11] Vezi definiții pe https://dexonline.ro/definitie/fenomen/definitii.

1. Coordonate spaţiale – zone/locuri

Mediile spaţiale (environments)[12] determină şi influenţează ţintele, activităţile în care se pot implica indivizii şi cine controlează locul (spaţiile au proprietari care pot fi relevanţi în rezolvarea unei probleme); identificarea şi etichetarea unui mediu facilitează comparaţia între medii, cu şi fără probleme (Clark şi Eck, 2016).

Tipuri de medii spaţiale:

- **rezidenţial** - locaţii în care locuiesc persoane – case, apartamente şi camere de hotel (locaţii fixe şi vehicule de agreement);
- **recreativ** - locuri unde persoanele se distrează - baruri, cluburi de noapte, restaurante, cinematografe, locuri de joacă, parcuri;
- **birouri** - locaţii de lucru – facilităţi guvernamentale şi de afaceri (există o interacţiune limitată între lucrători şi public; de regulă, accesul este restricţionat);
- **comerţul cu amănuntul -** locuri unde se realizează tranzacţii monetare – magazine şi bănci;
- **spaţii industriale -** locaţii pentru prelucrarea mărfurilor – fabrici, depozite şi unităţile de sortare (accesul publicului este limitat);
- **spaţii agricole -** locaţii pentru cultivarea culturilor şi creşterea animalelor;
- **spaţii educaţionale -** locuri de învăţare sau de studio – şcoli, colegii şi universităţi, biblioteci;
- **servicii umane -** locuri frecventate în momentele în care apar probleme – spitale şi centre de tratament, tribunale, închisori, secţii de poliţie;
- **legături publice -** rute care conectează toate celelalte medii – drumuri, autostrăzi, străzi, trasee, alei, locuri de parcare;
- **transport -** locaţii pentru mişcarea în masă a oamenilor – autobuze, staţii de autobuz, avioane şi aeroporturi, trenuri şi gări, feriboturi şi terminale de feriboturi;
- **spaţiu deschis/tranzitoriu -** zone care nu sunt desemnate pentru utilizare regulată – proprietăţi abandonate şi şantiere de construcţii.

[12] Ca semnificaţie extinsă, mediul se referă la un cadru spaţio-social unde se regăsesc persoane. Vezi definiţii bunuri şi servicii pe https://dexonline.ro/definitie/mediu/definitii

Analiza mediilor spațiale reprezintă identificarea și evaluarea mediilor fizice, pentru a înțelege modul în care acestea pot influența entități (ca proprietari/utilizatori), comportamente și desfășurarea de activități.

2. Coordonate temporale – trecut-prezent-viitor (momente-perioade):

Analiza coordonatelor temporale se reflectă în înțelegere detaliată a modului în care activitățile ilegale sunt organizate și executate în timp (cu momentele-perioadele de activitate intensă sau repaus). Analiza coordonatelor temporale se concretizează în:

- identificarea unor momente-perioade favorabile/selectate pentru desfășurarea de activități ilegale;
- înțelegerea de ce și cum unele activități se desfășoară într-un anumit interval de timp (când au loc și cât durează);
- monitorizarea timpului petrecut de persoane în anumite locuri sau alocat unor activități;
- identificarea momentelor semnificative/intense pentru anumite activități;
- stabilirea de pattern-uri și tendințe de comportament/activități;
- identificarea schimbărilor în comportamentul unei entități;
- anticiparea și prevenirea unor eventuale activități ilegale;
- identificarea momentelor în care diverse entități pot fi vulnerabile;
- identificarea momentelor critice în care structurile statului pot fi vulnerabile;
- identificarea momentelor cheie în desfășurarea activităților (aspect util în prevenirea și combaterea activităților ilegale).

Analiza coordonatelor spațiale și temporale are ca rezultat identificarea potențialelor vulnerabilități pentru a dezvolta strategii de intervenție, gestionare, prevenire sau contracarare.

Factori de activare a entităților

Factorii de activare a entităților se concretizează în: *mijloace de deplasare* (modalități de transport pentru persoane sau grupuri - mașini, microbuze, trenuri, avioane etc)*, mijloace de comunicare* (conversații personale, apeluri telefonice/video, mesaje text, e-mail, rețele sociale, într-un mod codificat/necodificat), *resurse relaționale* (prieteni, membri

de familie, colegi de muncă, factori de decizie, persoane care furnizează anumite bunuri şi servicii, forţa şi calitatea relaţiilor), *resurse financiar-materiale* (bani, obiecte de valoare, proprietăţi, echipamente), *acces* (spaţii private sau publice, facilităţi publice, informaţii, tehnologie, hrană, apă, adăpost, asistenţă medicală). Factorii de structurare a realităţii/ entităţilor sunt *pattern-urile, trend-urile, schimbările, asocierile şi fluxurile.*

1. Pattern-uri

Identificarea unor patternuri – tipare repetitive, recurente sau modele – se reflectă în înţelegerea (structurii) unor comportamente, activităţi şi procese[13] şi stabilirea tendinţelor, facilitând previziuni.

În contextul activităţilor ilegale, se identifică: frecvenţa şi regularitatea activităţilor ilegale; tiparele de acţiuni/comportamente pe anumite coordonate spaţio-temporale (locaţii şi momente); structura grupului şi ierarhia (tipurile de relaţii socio-profesionale); modul de operare şi organizare a activităţilor ilegale; modalităţile de comunicare între diverse entităţi; mijloacele de obţinere a resurselor financiare şi de plată pe plan intern şi extern; evoluţia şi schimbările în modul de desfăşurare a activităţilor în timp.

Analiza patternurilor facilitează structurilor de law enforcement/ informative să anticipeze mişcările viitoare şi să îşi coordoneze eficient resursele şi măsurile de prevenire şi contracarare (prin identificarea vulnerabilităţilor şi momentelor critice).

2. Trend-uri

Identificarea unor trenduri – evoluţie şi schimbări ale unor activităţi sau fenomene[14] – se reflectă în înţelegerea direcţiilor şi anticiparea unor eventuale ameninţări sau oportunităţi.

În contextul activităţilor ilegale, se fac evaluări referitoare la tipurile de bunuri şi servicii, volumul de tranzacţii ilegale, frecvenţa şi relevanţa unor activităţi.

Factorii incluşi în evaluarea tendinţelor activităţilor ilegale sunt următorii: *date istorice* (evoluţia istorică şi tendinţele din trecut, precum şi despre impactul măsurilor de prevenire/combatere)*; date demografice şi geografice* (componenţa grupărilor şi regiuni)*; date economice*

[13] Vezi definiţii pe https://www.britannica.com/dictionary/pattern.
[14] Vezi definiţii pe https://dexonline.ro/definitie/tendin%C8%9B%C4%83/definitii.

(implicaţiile financiare)*; date sociale şi culturale* (valori culturale, norme sociale, relaţii interpersonale)*; date tehnologice* (echipamente şi tehnologii)*; date legislative şi politice* (reglementări legale, strategii şi măsuri de prevenire/combatere).

Analiza trendurilor facilitează structurilor de law enforcement/ informative înţelegerea şi anticiparea evoluţiei şi schimbărilor unui fenomen sau activităţi, identificarea factorilor care le influenţează, astfel încât să se dezvolte măsuri eficiente de gestionare a eventualele ameninţări sau oportunităţi.

3. Schimbări

Identificarea unor schimbări – modificări semnificative ale coordonatelor spaţio-temporale ale activităţilor ilegale şi a modului de operare[15] – se reflectă în detectarea modificărilor în diverse comportamente/activităţi şi corelarea cu modificări ale măsurilor juridice, economice sau de securitate care au exercitat/exercită influenţe specifice, şi a modului în care se pot adapta la acestea grupări sau organizaţii.

Factorii interogativi incluşi în evaluarea schimbărilor aferente activităţilor ilegale sunt următorii: Ce schimbări majore au avut loc pe coordonate spaţio-temporale, juridice, economice, tehnologice şi de securitate (modificări legislative, evoluţii economice, inovaţii tehnice)?; Care sunt consecinţele acestor schimbări asupra activităţilor ilegale (oportunităţi şi riscuri)?; Cum au reacţionat diverse entităţi la schimbări (adaptarea strategiilor sau menţinerea modului de operare)?; Care sunt tendinţele/direcţiile generale ale activităţilor ilegale (creştere sau scădere a activităţii, schimbări în domeniile de acţiune)?; Ce alte evenimente sau schimbări pot afecta activităţile ilegale în viitorul apropiat şi cum ar putea să influenţeze evoluţia acestora (modificări ale costurilor pentru bunuri şi servicii, pentru transport, evoluţii ale pieţei, apariţia altor jucători pe piaţă)?

Analiza schimbărilor facilitează structurilor de law enforcement/ informative examinarea şi înţelegerea unor factori care determină schimbările semnificative şi evaluarea eficacităţii măsurilor de prevenire şi contracarare (cu identificarea unor noi oportunităţi de intervenţie).

---

[15] Vezi detalii pe https://www.collinsdictionary.com/dictionary/english/change.

4. Asocieri

Identificarea unor asocieri – relaționare, acțiune comună pe baza anumitor principii pentru atingerea unor obiective[16] – se reflectă în înțelegerea conexiunilor dintre persoane, grupuri, organizații, locații și tipuri de activități (pentru de a determina dacă sunt semnificative sau sunt coincidențe).

În contextul activităților ilegale, se identifică persoane/rețele și se determină modul în care colaborează și interacționează într-un anumit context.

Factorii pentru analiza asocierilor pot include: *entități din rețea* – persoane, grupuri, organizații (identificarea și definirea entităților, a relațiilor dintre acestea); *relații intra/inter entități* (lideri, structură de putere, influență și ierarhie, cine deține informațiile, puterea și influența); *tipare de conexiuni* (comunicare, colaborare, tranzacții financiare sau alte tipuri de interacțiuni); *fluxuri de bani și utilizarea de alte resurse* (cine controlează accesul la resurse); *tiparele comportamentale* (frecvența și tipul de interacțiuni sau tranzacții financiare); *comportamente atipice/suspecte* (relații neobișnuite sau tranzacții financiare suspecte); *legături cu alte rețele* (tipuri de legături dintre rețele, modul în care aceste legături influențează activitățile și comportamentul din rețea, implicarea în alte activități ilegale).

Analiza asocierilor facilitează structurilor de law enforcement/ informative înțelegerea complexității și interdependenței unor elemente (frecvența cu care unele elemente apar împreună și a relațiilor/ corelațiilor semnificative), descoperirea de structuri ascunse, modele și tendințe, astfel încât să se poată interveni în mod eficient pentru stoparea sau diminuarea activităților ilegale.

5. Fluxuri

Identificarea unor fluxuri – circulația continuă de bunuri, servicii, bani, informații în cadrul unei succesiuni de secvențe dintr-un proces, sub forme de organizare cu divizare specifică, și raportată la cantitate și timp de transmitere[17] – se reflectă explicarea și interpretarea activităților/ rețelelor de obținere și diseminare, a valorii asociate, a beneficiarilor și

[16] Vezi definiții pe https://dexonline.ro/definitie/asociere/definitii.
[17] Vezi definiții pe https://dexonline.ro/definitie/flux/definitii.

motivațiilor (Banc, n.d.). În contextul activităților ilegale, se identifică principalele entități implicate, structura ierarhică și rolurile, locurile și volumul de tranzaționare și tranzit, destinația și beneficiarii finali.

Factorii pentru analiza fluxurilor sunt următorii: bunurile tangibile/ intangibile și serviciile; principalele persoane implicate în fluxuri; structura ierarhică a organizației sau grupului care derulează fluxurile, precum și eventualele paliere pe care se desfășoară acestea; modalitatea în care se derulează fluxurile și rolurile entităților implicate; persoanele care fac legătura cu alte organizații în cadrul fluxurilor; locurile de plecare, tranzit, destinație și beneficiari finali, din punct de vedere cantitativ și calitativ; soliditatea legăturilor dintre entități, din perspectiva importanței și dinamicii fluxurilor; elementele asupra cărora se poate acționa pentru a se stopa fluxuri, perturba activități și eventual destructura rețele.

Analiza fluxurilor facilitează structurilor de law enforcement/ informative obținerea unei imagini de ansamblu asupra activităților ilegale sau suspecte, cu identificarea modurilor de operare și a elementelor cheie ale acestora, pentru a putea lua măsuri de stopare sau perturbare a fluxurilor și destructurare a rețelelor infracționale (Bărbuță și Marin, 2014a, p. 82).

Factori operativi

Factorii operativi sunt *amenințările, vulnerabilitățile, riscurile.*

1. Amenințarea reprezintă "acțiuni, fapte sau stări de fapt, capacități, strategii, intenții ori planuri ce pot afecta valorile, interesele și obiectivele naționale de securitate și/sau sunt de natură să pună în pericol direct sau indirect securitatea națională, prin afectarea funcționării normale a instituțiilor statului, a vieții și integrității fizice a cetățenilor și a organizării comunităților umane" (*Ghidul strategiei naționale de apărare a țării pentru perioada 2015-2019*, 2015, p. 8).

2. Vulnerabilitatea este "o deficiență funcțional-sistemică/ structurală care poate fi exploatată sau poate contribui la materializarea unei amenințări sau risc, determinând slăbirea capacității statului de a diminua impactul evenimentelor cu potențial de afectare gravă a funcționării normale a instituțiilor sale, a vieții și integrității fizice a cetățenilor și a organizării comunităților umane, precum și a capacității

de protejare, apărare şi promovare a valorilor, intereselor şi obiectivelor naţionale de securitate" (*Ghidul strategiei naţionale de apărare a ţării pentru perioada 2015-2019*, 2015, p. 10).

3. Riscul se constituie în "probabilitatea de producere/manifestare a oricărui eveniment, situaţie, condiţie cu potenţial de manifestare incert, a cărui concretizare ar conduce la afectarea în orice mod a funcţionării normale a instituţiilor statului, a organizării şi funcţionării comunităţilor umane, precum şi a vieţii şi integrităţii fizice a cetăţenilor, într-o împrejurare dată sau context determinat" (*Ghidul strategiei naţionale de apărare a ţării pentru perioada 2015-2019*, 2015, p. 9).

Factorul de investigare-rezolvare

Factorul de investigare-rezolvare este *problema.* Analiza unei probleme – aspect important neclar, complicat şi care devine o dificultate care trebuie explicată şi rezolvată pentru a se obţine un anumit rezultat, constituindu-se o sarcină care necsită o soluţionare (imediată)[18] – se reflectă în culegerea[19] şi evaluarea (interpretarea) datelor au ca obiective *înţelegerea* cauzelor, factorilor contributori, finalităţii şi consecinţelor/efectelor manifestării problemei, respectiv *identificarea* trendurilor sau pattern-urilor ce implică incidente, locaţii şi persoane (Bărbuţă şi Marin, 2014, pp. 143-144). Analiza unei probleme facilitează structurilor de law enforcement/informative: identificarea a ceea ce este deja cunoscut; unde pot fi găsite date pentru a umple golurile de

[18] Vezi definiţii pe https://dexonline.ro/definitie/problema/definitii.

[19] În contextul factorului de investigare vs problemă, punctăm dinamica "noilor provocări de securitate al căror element fundamental este dimensiunea umană în care HUMINT devine cheia", vezi detalii pe https://www.qmagazine.ro/humint-lectii-invatate-din-razboi/. Evidenţiem explorarea operativ-informativă (educing information) care integrează metodele/tehnicile, procesele, mecanismele, factorii prin care se eficientizează obţinerea, detalierea, corelarea, verificarea şi aprofundarea, prin relaţionare interpersonală, a datelor de interes operativ – în general, cumulează interviurile de securitate, interogatoriul/interviul pentru intelligence/ interviul investigativ, debriefing-ul. Prin HUMINT se creează avantaje de natură politico-economică şi militară (prin accesul la obiective, intenţii, planuri operaţionale şi strategice), respectiv pot fi documentate activităţile grupărilor teroriste şi ale celor de criminalitate organizată. Vezi detalii pe What Is HUMINT, How Does It Work & Why Do We Need It?, disponibil la https://isotecsecurity.com/humint/

cunoaştere; cum ar putea fi obţinute astfel de date; semnificaţiile care poate fi decupate (James, 2016, p. 27).

Fişa analitică tip interogativ-evaluativă – problemă (Bărbuţă şi Marin, 2014, p. 172 şi 190):

- ☐ CINE?: Cine este făptuitorul sau persoana identificată în urma derulării analizei; Cine este responsabil de apariţia problemei; Cine a fost martor la evenimente sau la incidente; Cine sunt ţintele;
- ☐ CE?: Ce anume au făcut, fac sau vor face persoanele; Ce categorii de fapte s-au comis; Ce rutine pot fi identificate; Ce relaţii sunt între faptele înregistrate şi alte variabile (timp, spaţiu etc); Ce cauze au determinat apariţia acestei probleme; Ce trenduri prezintă problema;
- ☐ CÂND?: Când s-au petrecut faptele sau când au fost descoperite indicii privind comiterea acestora (intervalul);
- ☐ UNDE?: Unde s-au petrecut faptele ori au fost găsite indicii referitoare la săvârşirea lor; Unde se afla sau de unde a venit persoana; Tipul locaţiilor, denumirea acestora şi zona în care s-au petrecut incidentele;
- ☐ DE CE?: Motivaţia comiterii faptelor sau scopul urmărit; Există şi alte variabile relaţionate cu diverse situaţii, pentru a se putea evidenţia eventuale conexiuni ori legături;
- ☐ CUM?: Cum a apărut problema; Cum anume s-a acţionat pentru comiterea faptelor; Cum se manifestă sau cum s-a manifestat această problemă în decursul unei perioade de timp.

Subsumat situaţiei operative şi problemei există **contextul,** care reprezintă "o condiţie, conjunctură, situaţie specifică, circumstanţă, stare de lucruri într-un anumit moment, un ansamblu/concurs de împrejurări[20] care însoţesc/în care se produce un fenomen/eveniment"[21].

Prin analiza contextului se evidenţiază şi interpretează diverse aspecte relevante pentru un anumit fenomen (eveniment). Componentele analizei unui context sunt următoarele:

---

[20] Definiţii împrejurare – situaţie în care se află cineva şi circumstanţă/întâmplare – situaţie în care are loc un eveniment oarecare, disponibile la https://dexonline.ro/definitie/%C3%AEmprejurare/definitii.

[21] Vezi definiţii pe https://dexonline.ro/intrare/context/12611/definitii.

a) *cadrul general* (background-ul/antecedentele şi pattern-urile de tip istoric, social, cultural, economic, decizional etc care au influenţat/influenţează starea actuală).
b) *entităţile implicate* (identificarea capabilităţilor, resurselor, motivaţiilor, intereselor şi perspectivelor pentru a se evalua cum influenţează/cum pot fi influenţate)
c) *factori interni/externi* (tendinţe locale/globale – politice, economice, sociale, culturale, militare, tehnologice etc).
d) *conexiuni şi interacţiuni* (stabilirea şi studierea relaţiilor dintre diferite entităţi, pentru a se evalua dependenţele şi dinamica puterii – conflicte sau cooperări).
e) *constrângeri şi resurse* de natură financiară, umană, juridică, materială etc.
f) *consecinţe* (identificarea riscurilor şi oportunităţilor, respectiv şi a potenţialelor compromisuri).

A descifra condiţiile şi circumstanţele asociate unei situaţii/ eveniment – contextul – se reflectă în fundamentarea unor măsuri, reacţii, decizii, strategii eficiente.

Fişă analitică tip interogativ-evaluativă – context

- Care sunt circumstanţele actuale aferente fenomenului/ evenimentului/situaţiei/problemei?
- Care sunt principalele entităţi interesate/implicate în context?
- Există un background/antecedente de tip istoric, social, cultural, economic, juridic, diplomatic etc care infuzează contextul actual?
- Care sunt aspectele sociale, economice, politice, culturale etc actuale relevante pentru context?
- Care sunt factorii cheie sau variabilele – persoane, reţele, medii, acţiuni, produse, servicii, repere spaţio-temporale – care determină contextul?
- Care sunt factorii interni sau externi de tip grupal/organizaţional/ statal care influenţează contextul?
- Care sunt consecinţele sau implicaţiile potenţiale ale contextului pentru fenomen/situaţie/problemă?
- Există ameninţări sau oportunităţi specifice asociate contextului?
- Influenţează/cum influenţează contextul procesul de fundamentare a unor măsuri, reacţii, decizii?

O analiză eficientă implică examinarea contextului recent care a determinat/ influenţat evenimentul dar şi anticiparea posibilelor evoluţii, pentru că se pot identifica provocările şi oportunităţile şi se concretizează o atitudine pro-activă în ceea ce priveşte pregătirea pentru apariţia diferitor rezultate/efecte.

Realizarea obiectivelor unei analize raportată la situaţie operativă – problemă-context – presupune clarificarea următoarelor elemente (Bărbuţă şi Marin, 2014, p. 143-144)[22]: cine este implicat; ce s-a întâmplat anterior manifestării problemei; unde s-a manifestat ori se manifestă problema; ce alte lucruri se întâmplă sau nu se întâmplă în timp ce problema este prezentă şi îşi manifestă efectele; care sunt efectele ulterioare manifestării problemei şi care este frecvenţa/ relevanţa acestora; cine este afectat şi în ce constă prejudiciul; ce resurse sunt disponibile pentru rezolvarea problemei; se pot identifica în trecut probleme similare sau care au legătură cu problema actuală; se pot identifica în trecut răspunsuri/ abordări/ resurse viabile care au rezolvat probleme similare sau care au legătură cu problema actuală.

***

În concluzie, apreciem că *factorii constitutivi* (persoanele, reţelele, grupările – entităţile, activităţile, bunurile şi serviciile, piaţa, fenomenele/ evenimentele), *coordonatele pre-stabilite* (spaţiale şi temporale), *factorii de activare a entităţilor* (mijloace de deplasare, mijloace de comunicare, resurse relaţionale, resurse financiar-materiale, acces), *factorii de structurare* (pattern-urile, trend-urile, schimbările, asocierile şi fluxurile), *factorii operativi* (ameninţările, vulnerabilităţile, riscurile) (Găitan, 2020, p. 356) reprezintă un **model** (reprezentare grafică în figura 1) pentru înţelegerea situaţiei operative care reflectă legături de cauzalitate şi dinamica evolutivă a ameninţărilor, riscurilor şi vulnerabilităţilor, selectiv pe următoarele dimensiuni: informaţii, contrainformaţii şi securitate, apărare, ordine publică, economică şi energetică, tehnico-ştiinţifică, diplomatică, situaţii de criză şi protecţie civilă, mediul înconjurător-ecologie, educaţie, sănătate, administrativ-socială.

[22] Elementele reprezintă, de regulă, datele operative (datele brute, primare/date de primă sesizare) – date despre persoane (fizice, juridice), grupări, medii, organizaţii, situaţii, evenimente, contexte etc, care se referă la vulnerabilităţi, ameninţări, riscuri.

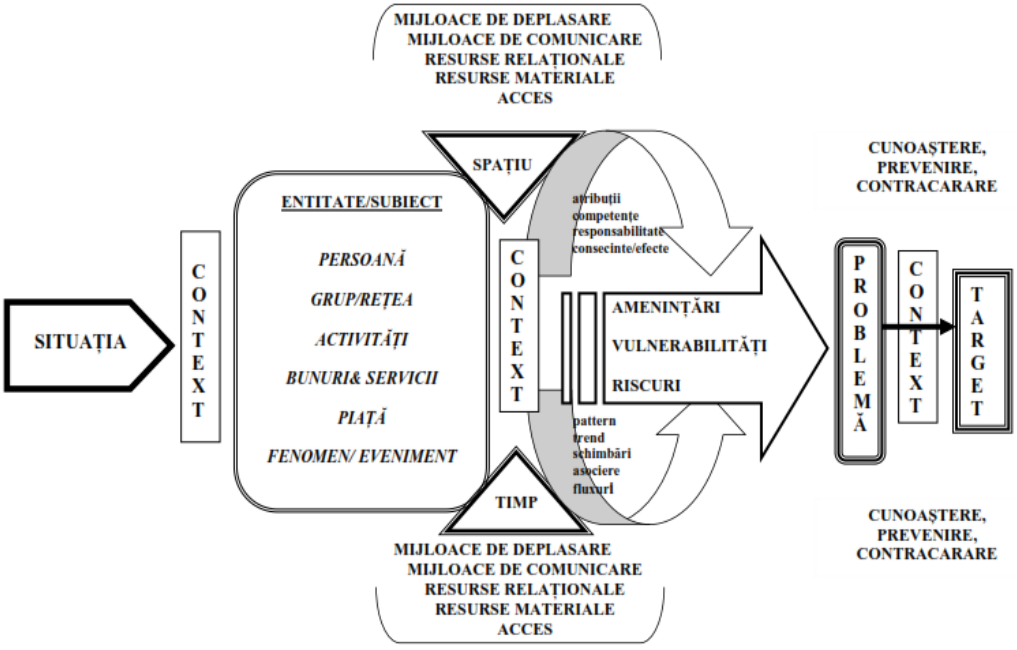


Figura 1: Model integrat al situaţiei operative
(Sursa: viziunea autorului bazată pe literatura de specialitate)

Referinţe bibliografice:

1. Alexandra Sarcinschi. (2005). *Omul – subiectul securităţii naţionale şi internaţionale,* în volumul *Provocări la adresa securităţii şi strategiei la începutul secolului XXI* (Universitatea Naţională de Apărare – Sesiunea de comunicări ştiinţifice cu participare internaţională – 14-15 aprilie 2005 – secţiunea: apărare şi securitate naţională) – disponibil la https://cssas.unap.ro/ro/pdf_carti/ provocari _ la_ adresa_securitatii_si_strategiei_2005.pdf

2. Bărbuţă Cristian-Gelu, Marin Floriana-Lucia. (2014). *Intelligence: o nouă revoluţie*, Craiova: Sitech.

3. Bărbuță Cristian-Gelu, Marin Floriana-Lucia. (2014a). *De la informație la intelligence,* Craiova: Sitech.

4. Clark, Ronald V., and John E. Eck. (2016). *Crime Analysis for Problem Solvers in 60 Small Steps.* Washington, DC: Office of Community Oriented Policing Services

5. *Intelligence și management strategic modern,* (2012). București: Editura Academiei Oamenilor de Știință din România

6. Florian Coldea, Niță Cristian. (2022). *Etică în intelligence – curs introductiv,* București: Editura ANIMV.

7. Liviu Găitan. *(2020). Secretele de dincolo de ușă. Secvențe din viață și memoria profesională și nu numai*, Arad: Concordia.

8. Panfil Banc. (n.d.). *Câteva aspecte referitoare la fluxurile și ciclurile financiare*, accesibil la http://www.oeconomica.uab.ro/upload/lucrari/820062/03.pdf

9. Radu Cristescu. (2000). *Spionajul și contraspionajul pe înțelesul tuturor. Mic dicționar al serviciilor secrete*, București: Evenimentul Românesc.

10. Ministerul Administrației și Internelor. Direcția Generală Organizare, Planificare Misiuni și Resurse. (2006). *Glosar de termeni din domeniul ordinii și siguranței publice*, București: Editura MAI.

11. *Strategia națională de ordine și siguranță publică 2023-2027*, România. MAI, disponibilă la https://webapp.mai.gov.ro/frontend/documente_transparenta/547_1679910354_Proiect%20SNSOP%202023-2027%20%20martie%202023.pdf

12. *Strategia națională de ordine și securitate publică 2017-2020,* Republica Moldova. disponibilă la https://gov.md/sites/default/ files/document/attachments/intr20_71.pdf

13. Traian Stambert, Gheorghe Dragu, Liviu Găitan. (2010). *Limbajul serviciilor secrete. Servicii de informații și de securitate*, București: Editura PACO.

14. Vasile Robu, Nicolae Georgescu. (2001). Analiză economico-financiară, București: ASE, disponibil la http://www.biblioteca-digitala.ase.ro/biblioteca/carte2.asp?id=113&idb=6

15. United Nations Office on Drugs and Crime (UNDOC, 2010). *Criminal Intelligence. Manual for Front-line Law Enforcement*, United Nations, New York.

16. *Ghidul strategiei naționale de apărare a țării pentru perioada 2015-2019*, disponibil la https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019

17. *Doctrina națională a informațiilor pentru securitate,* adoptată prin Hotărârea Consiliului Suprem de Apărare a Țării din 23 iunie 2004.

Wesite-uri:

https://www.manigordo.ro/index.php?option=com_glossary&letter=S&id=96&Itemid=113&lang=ro
https://isotecsecurity.com/humint/
https://dexonline.ro/definitie/leg%C4%83tur%C4%83/definitii
https://dexonline.ro/definitie/activitate/definitii
https://ro.economy-pedia.com/11031726-goods-and-services
https://invatatiafaceri.ro/diferente/diferenta-dintre-bunuri-si-servicii/
http://ec.utgjiu.ro/wp-content/uploads/2023/02/Microeconomie.pdf
https://dexonline.ro/definitie/pia%C8%9B%C4%83/definitii
https://dexonline.ro/definitie/eveniment/definitii
https://dexonline.ro/definitie/fenomen/definitii
https://dexonline.ro/definitie/realitate/definitii
https://dexonline.net/definitie-situa%C8%9Bie
https://dexonline.ro/definitie/Fapt
https://dexonline.ro/definitie/mediu/definitii
https://www.britannica.com/dictionary/pattern
https://dexonline.ro/definitie/tendin%C8%9B%C4%83/definitii
https://www.collinsdictionary.com/dictionary/english/change
https://dexonline.ro/definitie/asociere/definitii
https://dexonline.ro/definitie/flux/definitii

REVIEWS AND NOTES

Florica Dobre, *O istorie a CIE (Centrul de Informaţii Externe): octombrie 1978 - decembrie 1989: structuri, cadre, obiective şi metode*, Editura Glasul istoriei, Bucureşti, 2022, vol 1, p. 675 şi vol 2 p. 630, prezentare de Codruţ LUCINESCU

Arhivist şi cercetător de carieră cu activitate de peste 20 de ani la CNSAS, Florica Dobre, autorul celor două volume *O istorie a CIE (Centrul de Informaţii Externe): octombrie 1978 – decembrie 1989: structuri, cadre, obiective şi metode*, s-a preocupat în mod repetat de dezvăluiri documentare din sfera istoriei fostelor instituţii de forţă din perioada comunistă. Având la dispoziţie arhivele gestionate de această instituţie, a fost, de-a lungul carierei sale de cercetător acreditat şi împreună cu alţi colegi din instituţie, coordonator al unor volume precum: *Distrugerea elitei militare sub regimul ocupaţiei sovietice în România*, vol. 1, 2000 şi vol. 2, 2001, Bucureşti, Editura Institutul Naţional pentru Studiul Totalitarismului; *Trupele de Securitate (1949-1989)*, Editura Nemira, Bucureşti, 2004; *Securitatea. Structuri, cadre, obiective şi metode*, vol. 1 şi vol. 2, Editura Enciclopedică Bucureşti, 2006.

Cele două volume de documente dedicate Centrul de Informaţii Externe redau în mod sistematic şi organizat, pe parcursul a peste 1200 de pagini, o serie de materiale din perioada octombrie 1978 – decembrie 1989 declasificate de către Serviciul de Informaţii Externe – documente, fişe personale, decrete de organizare şi funcţionare a structurilor de informaţii externe, buletine informative –, aflate astăzi în arhiva CNSAS. Documentele restituite suplimentează şi validează informaţiile conţinute în alte volume despre serviciile de spionaj autohtone, precum *Ultimul curier ilegal* (Cornel Nemetzi), *Reqviem pentru spioni* (Gheorghe Dragomir), *Mihai Caraman – un spion român în Războiul Rece* (Florian Banu) ori, mai

noua apariţie editorială, *Fantomele prezentului* (Cornel Biriş), adăugând nota de obiectivitate dată de studiul ştiinţific al arhivelor care, posibil, le lipseşte în oarecare măsură lucrărilor memorialistice, caracterizate de autenticitatea conferită prin participarea nemijlocită a autorului la evenimente, dar însoţite de un potenţial subiectivism.

Lucrarea *O istorie a CIE* este validată printr-o prefaţă scrisă chiar de Generalul Gheorghe Dragomir (*alias*, în decursul timpului Vlad Bolintineanu, Spătaru Vlad, Sabău Vlad şi Dragu Gheorghe), unul dintre lucrătorii de informaţii externe prezentaţi în carte, care a ocupat la momente diferite inclusiv poziţia de şef al unor unităţi din cadrul CIE şi care a devenit apoi în perioada 1990-1992 adjunct al directorului SIE. Dincolo de controversa „desconspirărilor ilegale" la care a dat naştere lucrarea autoarei[1], cele două volume sunt de importanţă pentru istoria Intelligence-ului românesc dintr-o perioadă complexă şi controversată.

O istorie a CIE se remarcă prin efortul depus de cercetător pentru ordonarea şi „decriptarea" materialului arhivistic, acesta fiind redactat în original într-un limbaj mai puţin accesibil specific unui serviciu de informaţii externe. Acolo unde nu a reuşit să descifreze documentele, coordonatoarea volumului a avut ideea foarte inspirată de a cere Serviciului de Informaţii Externe – din poziţia acestuia de păstrător legal al arhivelor clasificate ale CIE – clarificări suplimentare, pe care în câteva cazuri le-a şi primit aşa cum ea însăşi recunoaşte: „Pe parcursul studierii dosarelor SIE, constatând ca ofiţerii apăreau în documente cu mai multe nume, am propus conducerii CNSAS să avizeze transmiterea către SIE a mai multor adrese cu numele ofiţerilor de informaţii externe nominalizaţi în dosare şi ale căror fişe de evidenţă se cereau a fi predate. Astfel, în baza documentelor întocmite de mine s-au predat peste 40% din totalul fişelor de evidenţă existente azi în arhiva CNSAS. (…) Coroborate şi completate cu alte informaţii, aceste documente au stat la baza întocmirii a 234 de fişe de cadre." (vol. 1, p. 19) În lumina afirmaţiilor sale, este confirmat faptul că CIE, asemeni altor structuri similare, şi-a protejat lucrătorii schimbându-le numele ori i-a implantat în mediile-ţintă

[1] Vezi detalii despre procesul „desconspirărilor ilegale", proces solutionat cu respingerea acuzaţiilor, în presă: https://ziare.com/ristea-priboi/proces-ristea-priboi-spioni-die-divulgare-secrete-de-stat-cnsas-motivare-1808738.

fabricându-le biografii şi legende credibile, aceste acţiuni fiind de importanţă în munca de intelligence.

Mai importantă decât materialul documentar în sine, structurat şi pus la dispoziţia cititorului, este cheia de decriptare pe care coordonatoarea volumelor o elaborează şi ne-o oferă sub forma părţilor introductive precum: *Lista cu abrevieri*, *Lista de termeni şi expresii codificate* şi *Tabelul cu reşedinţele şi denumirile grupelor operative externe*. Aceasta face posibilă înţelegerea anumitor pasaje, în special a telegramelor şi a notelor-raport transmise de către lucrătorii aflaţi la post în străinătate, care altfel ar rămâne opace pentru cititorul comun. Iată un exemplu elocvent: „Suporterul *TACHE*, de la redacţia Goleşti, a fost suplinit de mai multe ori de un reporter voilean, în scop de prelucrare şi diagnosticare proiectivă. Conformându-se indicaţiilor primite din Studio, suporterul a evitat suplinirile cu reporterul voilean şi a imprimat un caracter strict oficial statisticilor cu el." (vol. 1, p. 126) Acest text inteligibil pentru noi, devine după traducerea lui pe baza indicaţiilor din *Lista de termeni şi expresii codificate*: „Sursa Tache, de la grupa operativă externă Geneva, a fost contactată de un diplomat american, în scop de prelucrare şi exploatare informativă. Conformându-se indicatiilor primite din Centrală, sursa a evitat contactele cu diplomatul american şi a imprimat un caracter strict oficial relaţiei cu el."

Obiectivismul caracteristic cercetătorului profesionist însoţeşte întreaga lucrare fiind penetrat punctual de pasaje din care reiese un oarecare respect al coordonatoarei celor două volume pentru lucrătorii de informaţii externe: „Elita Securităţii – aşa ar trebui consideraţi cei care au lucrat în structurile de informaţii externe. Absolvenţi de instituţii de învăţământ superior şi buni specialişti în domeniile lor de activitate, cunoscători a două sau mai multe limbi străine, au fost profesionişti în arta spionajului." (vol. 1, p. 67). Datele statistice prezentate în volumul 1 ne ajută să ne formăm o imagine a profilului lucrătorului de informaţii externe: „În privinţa studiilor de stat, de specialitate şi militare, 98% din totalul ofiţerilor absolviseră învăţământul superior, fiind pregătiţi în următoarele specialităţi: 24,31% ingineri, 19,80% economişti, 33,81% jurişti, 17,87% profesori (majoritatea de limbi străine), 1,93% medici, iar restul alte specialităţi" (vol. 1, p. 41). În alt pasaj se specifică faptul că:

„70% sunt cunoscatori de limbă engleză, 40% cunosc două limbi de circulaţie internaţională." (vol. 1, p. 41) Astfel, documentele restituite prin efortul cercetătorilor de la CNSAS dovedesc faptul că activitatea de informaţii externe nu s-a redus la monitorizarea diasporei româneşti ci la o complexitate de misiuni menite a promova interesele României în străinătate, misiuni precum cunoaşterea atitudinii clasei politice din spaţiile de interes cu privire la ţara noastră şi susţinerea economiei naţionale prin obţinerea de elemente tehnico-ştiinţifice valoroase supuse embargoului sau care necesitau efort valutar consistent.

În încheiere, merită redate două pasaje care ne fac să ne întebăm oare câte forme poate să îmbrace un adversar care acţionează în spaţiul euro-atlantic, pornind de la premisa că metodele utilizate de CIE acum mai bine de 30 de ani nu sunt nici originale şi nici unice: „Cadrele care desfăşurau activitate la instituţiile de acoperire din ţară: se documentau asupra ţării în care urmau să meargă la post; îşi însuşeau şi perfecţionau cunoştinţele necesare exercitării funcţiei de acoperire ... ." (vol. 1, p. 41) şi „Cadrele din exterior îşi desfăşurau activitatea sub acoperirea de diplomaţi, funcţionari internaţionali, reprezentanţi economici, specialişti, ziarişti, bursieri sau sub alte acoperiri." (vol. 1, p. 41) Astfel, cele două volume pot contribui la descifrarea bazelor activităţii de intelligence ale pleiadei de spioni ruşi identificaţi în ultimii ani acţionând cu identităţi şi cetăţenii fabricate, multiplele cazuri de diplomaţi expulzaţi sub suspiciunea de spionaj ne fac să credem că acele metode nu sunt depăşite şi încă sunt utilizate. În acest sens, lucrarea îi ajută pe toţi cei interesaţi să-şi contureze o idee asupra complexităţii muncii de informaţii externe, începând cu identificarea, atragerea şi pregătirea lucrătorului până la conspirarea intereselor, acţiunilor şi resurselor unei structuri de Intelligence.

ACADEMIC FOCUS

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 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 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 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:

- 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 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 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 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.

Funded by
the European Union

INSET
CrItical Studies in INtelligence, Technologies, and SEcuriTy Governance (01.11.2022 – 30.06.2024)

INSET is an ERASMUS Mundus Design Measures project developed by a consortium of three universities: Mihai Viteazul National Intelligence Academy (Romania), University of Malta (Malta) and University Rey Juan Carlos (Spain) and financed by the European Commission (ERASMUS-EDU-2022-EMJM-DESIGN, code 101081354).

The aim of INSET is to develop a **joint master's program in Critical Studies in Intelligence, Technologies, and Security Governance**. The focus is on developing complex and interdisciplinary competences which are needed in understanding the dynamics of the 21st century world which is increasingly technology-based, hostile from a security perspective, and highly volatile.

INSET advances an inter- and multidisciplinary approach that combines critical studies in intelligence, security governance and technologies while bridging these areas of study and transfers specialized knowledge and competencies from specialists and practitioners in intelligence and security towards the civil society.

INSET joint MA programme's distinct novelty emerges from the following objectives:

1. it brings an interdisciplinary and multidisciplinary approach, which intersects the several concentrations under security

science: critical studies in intelligence, security governance, technologies;

2. it applies a critical approach to address contemporary security challenges and build a resilient security culture;
3. it is structured in a way that can be understood and assimilated by a wide variety of students, with different backgrounds: media studies, law, technology, political sciences, sociology, intelligence and security studies;
4. it goes beyond addressing these study areas in a disparate and segmented fashion, transversally focusing on their intersection, on their convergence, and on the manner in which they can synergically solve real societal problems.

INSET joint MA programme addresses the following educational gaps:

1. the need for a common European academic framework to assess security risks through technologically-driven intelligence production;
2. the underrepresentation of interdisciplinary master programs linking intelligence studies, security governance and technologies;
3. the rapid and recent evolution of perspectives on intelligence and security from traditional to more critical, interdisciplinary and reflexive ones;
4. the need to link intelligence studies and technological developments to society at large and to develop civil societies' abilities to analyse data, understand the functionality of technology, develop their digital competences;
5. the missing tools in addressing disinformation campaigns, part of hybrid warfare, that are shaping and reshaping democratic systems and affecting good governance practices, with little understanding or control from civil society.

As a **joint transnational and inter- and multidisciplinary master's program, INSET** encourages the internationalization of education via critical approaches to security issues and increases the capacity of partners to deliver joint educational programs. By providing a common framework and support for networking, it fosters academic cooperation among partners and, accordingly, it enhances the partners' capabilities to modernize their curricula and teaching practices. In line with the recent developments of both theoretical approaches (e.g. critical intelligence studies) and also the unprecedented technological challenges, the program aims to develop cutting-edge and labour market attractive skills for BA graduates with different backgrounds (e.g. law, technology, social and political science, intelligence, media studies). By providing academic excellence, INSET designs and implements the mechanisms needed for the delivery and functioning of a joint master's program.

The consortium is currently developing the organizational documents and the curriculum for the **joint master's programme INSET** with a view to enrolling the first cohort of students in the autumn of 2025. More information is available on the project website.

Erasmus+ Mobility Projects at "Mihai Viteazul" National Intelligence Academy

Erasmus+ KA103 mobility projects are implemented within „Mihai Viteazul" National Intelligence Academy (MVNIA). The projects are funded by the European Commission, through the National Agency.

The objectives pursued by MVNIA within the the two mobility projects were in line with the specific objectives of Key-Action 1. Therefore, the Academy sought to:

- Support students in order to improve their knowledge, skills and competences;
- Favour quality improvement, excellence in innovation and internationalization by intensifying transnational cooperation with other higher education institutions and training centers;
- Improve the international dimension of education and professional training by promoting mobility and cooperation between higher education institutions;
- Increase the capacity to offer study programmes that better meet the needs of the students.

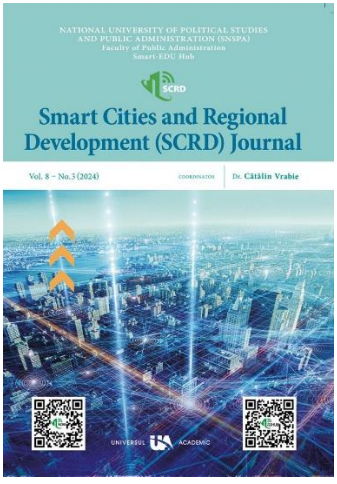
The mobility of staff and students sets the premises for improving professional knowledge and experience, developing linguistic and intercultural skills, as well as strenghtening European identity through the promotion of common values. Collectively, the 2 projects encompassed a number of 8 beneficiaries, students and professors alike, who took part in different tyes mobilities, as follows:

- 4 training mobilities
- 2 traineeships
- 1 teaching mobility
- 1 study mobility

MVNIA embraces cooperation and recognizes the importance of belonging to university networks for the development of competitiveness and institutional modernization. For this reason, strenghtening existing partnerships and starting new projects are objectives of utmost importance in the process of institutional internationalization. Fortunately, the Erasmus programme has put at MVNIA's disposal all the mechanism needed to achieve this goal. As a result, throughout the implementaion period, the Academy has signed three new inter-institutional agreements with the following institutions: University of Malta, the Jagiellonian University in Krakow and Matej Bel University in Banska Bystryca.

Even though the two projects have been completed, the Academy will continue to disseminate and exploit their results in new projects, scientific publications, and by developing new study programmes.

SMART CITIES AND REGIONAL DEVELOPMENT JOURNAL
ISSN: 2537-3803,
ISSN-L: 2537-3803,
ISSN online: 2821-7888



The *Smart Cities and Regional Development Journal* is built by the Smart-EDU Hub within The Faculty of Public Administration, National University of Political Studies and Public Administration, Romania. This presentation is an invitation to innovators, thinkers, and pioneers in Smart City Studies, and its aims is to propose the following principles.

Embrace the Future of Urban Living: Contribute to the SCRD Journal: A smart city is not just an urban area; it is a vibrant, living entity. At the *Smart Cities and Regional Development (SCRD) Journal*, we recognize the dynamic and evolving nature of smart cities – likening them to living organisms, with their complex and interconnected systems. This journal is your platform to explore, innovate, and share insights on this fascinating and crucial field.

Explore the Anatomy of Smart Cities: Delve into the intricate networks that form the backbone of smart cities. From transportation systems – the lifelines akin to circulatory systems, to educational and administrative institutions – the brains, every aspect of urban living is ripe for exploration and innovation.

Address Challenges, Celebrate Triumphs: While acknowledging the imperfections and challenges of urban spaces, the SCRD Journal is committed to showcasing successful smart city projects and innovative solutions. Share your experiences in transforming landfills, dilapidated structures, and underprivileged neighborhoods into vibrant, functional, and inclusive spaces.

A Platform for Cutting-Edge Research: The SCRD Journal is more than a publication, it's a beacon for the latest advancements in smart technologies. We cover a spectrum of topics, including virtual reality, augmented reality, artificial intelligence, and beyond. Your research and findings will guide global communities in adopting and integrating these technologies for the betterment of urban life.

Collaborate, Learn, and Inspire: Join a community of scholars, practitioners, and policymakers. Whether you are documenting the stages of development, sharing insights on innovation, or presenting results from prototype testing, your contribution will serve as inspiration and a practical guide for others.

Stay Ahead in a Rapidly Evolving Field: In an ever-changing technological landscape, the SCRD Journal is your go-to source for staying updated with the latest trends and breakthroughs in smart city development.

We invite authors, researchers, and practitioners in the fields of Smart Cities studies to contribute to the SCRD Journal. Share your insights, research, and visionary ideas. Together, let's shape the future of smart, sustainable, and resilient urban living. Be a part of the SCRD Journal – where your ideas and innovations pave the way for smarter, more sustainable cities.[1]

[1] We thank Professor Cătălin Vrabie for the presentation. Please see more details about the journal on *www.scrd.eu.*

CALL FOR PAPERS *ROMANIAN INTELLIGENCE STUDIES REVIEW*

"Mihai Viteazul" National Intelligence Academy 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 five weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 33 and 34 and which is scheduled to be published on June and December, 2025.

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: **animv.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.**